JOHANNES KEPLER
UNIVERSITY LINZ

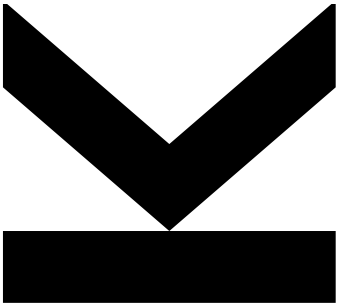
Submitted by
Christian Voglhuber

Submitted at
Institute of Networks and Security

Supervisor
Assoc. Prof. Mag. Dipl.-Ing. Dr. Michael Sonntag

May 2018

Security attacks and countermeasures in DOCSIS networks



Master Thesis
to obtain the academic degree of
Diplom-Ingenieur
in the Master's Program
Computer Science

JOHANNES KEPLER UNIVERSITY LINZ
Altenbergerstraße 69
4040 Linz, Österreich
www.jku.at
DVR 0093696

Abstract

This thesis focuses on the security aspects of cable networks. DOCSIS is a speficiation which is used by many cable operators to offer data services, like internet access, over existing TV-cables and architectures. The functionality and features of DOCSIS are described and security properties are evaluated. Moreover, a test system is deployed to simulate passive and active attacks. Those results are used to eliminate the vulnerabilities and problems of the DOCSIS network by securing the involved parts. Issues of the data encryption, authentication of modems, and provider headend equipment are presented. A case study reveals the state of security of two Austrian cable operators. Thereby many issues and vulnerabilities are detected, by merely passively sniffing the signals of a typical television port.

Kurzfassung

Diese Arbeit beschäftigt sich mit der Sicherheit von Kabelnetzwerken. DOCSIS ist eine Spezifikation, welche von vielen Kabelbetreibern verwendet wird um Datendienste, wie etwa Internetzugang, über vohandene TV-Kabel und Strukturen anbieten zu können. Die Funktion und Architektur von DOCSIS wird beschrieben und sicherheitsrelevante Eigenschaften aufgezeigt. Weiters wird ein Testsystem eingerichtet, um Angriffe in DOCSIS Netzwerken zu simulieren und zu identifizieren wie mögliche Probleme behoben werden können. Attacken auf die Datenverschlüsselung, Authentifizierung der Modems und der Provider-Kopfstation werden eruiert. Eine Fallstudie untersucht die Sicherheit von zwei österreichischen Kabelbetreibern. Dabei wurden viele Probleme, nur durch passives empfangen der Signale auf einem handelsüblichen TV-Anschluss aufgedeckt.

Contents

Chapter 1.

Introduction

Cable Television networks were developed to supply many people with the ability to watch TV cheaply. Since the first development and construction of a Community-Antenna-Television (CATV) system in 1948, the industry in connection to this technology has grown rapidly. Providers of such systems supply customers not only with pure TV reception, but they also offer Triple-Play solutions (Voice, Video, and Data) to end- and business-customers to compete with other companies and their technologies (like DSL).

Traditional Cable-TV-systems use a common medium, also known as shared-medium. Therefore, each subscriber receives the same information. At the beginning of the Internet success, it was clear that also private subscriber wanted the technology to surf the web. The cable companies decided to investigate on this, to be competitive and offer internet access via their CA-TV-Systems. To enable this, the research began to develop a technology to transmit data in both directions via the common media, which resulted in lots of proprietary product solutions. The main problem in the first place was to enable a bi-directional communication to the customers, which means that they can also transmit data and send it back to the provider. The first systems used a (Dial-Up) telephone line to make this transmission of data at the subscriber possible, and the reception was enabled via the normal CATV-System. This solution was not practical and the prices were too high, because of the extra telephone costs. At the time of the DSL technology development it was clear that there must be a practical solution to deliver high-speed internet access to the regular Cable-TV subscriber. Therefore, an open market for CATV data equipment has to be established to shrink the hardware prices and to make different vendors work together [54]. The industry developed the Data Over Cable Service Interface Specification (DOCSIS), to enable high-speed data communication over Cable-TV-Networks, which has the goal to deliver internet access to the Cable-TV subscribers. [10]

One of the biggest problems of CATV-Systems is the usage of a common media. Each subscriber receives all information. The result of such an architecture is very problematic regarding security. The requirements for securing this system are comparable with WiFi

networks (IEEE 802.11), but the attack range is much bigger because whole cities can be harmed. Therefore, a security concept has to be implemented, which makes sure information can only be sent and received at the corresponding device.

1.1. Motivation

The motivation for the work is mainly to show CATV (community antenna television) based data communication and their problems, especially regarding data privacy and security. Due to the fact that CATV uses a common media for all subscribers, the data communication needs to be protected against attacks (like eavesdropping). Big Providers, like KabelDeutschland, had big difficulties in the past to make their networks secure [1]. Moreover, some techniques of DOCSIS are also used by other technologies, like WiMAX (Worldwide Interoperability for Microwave Access) and PON (Passive Optical Network). Therefore, also those technologies inherit some properties of DOCSIS.

1.2. Task description

The thesis has the goal to primarily develop a lab environment for a DOCSIS network and to analyze the security problems and their countermeasures. Moreover, it gives a deeper insight into the protocol, especially the security-related considerations in DOCSIS. The second goal is to describe the DOCSIS protocol and the cable television (CATV) architecture and to evaluate the security measurements used by providers at the moment.

1.2.1. Practical

One major part of the work is to build a fully working DOCSIS network as lab environment (not fully blown like a live system). This involves some components, which are shown in figure 1.1, correctly wired together and properly configured. The parts can be split into these categories:

- Cable plant: All the physical parts need to be connected. A cable plant is usually a combination of modulators, demodulators, combiners, splitters, and amplifiers. To build the lab environment, all parts of the plant must be aligned together to match the RF (Radio frequency) parameters.
- Cable modem termination system (CMTS): This unit is the counterpart of the connected cable modems. It requires a configuration according to the physical plant properties (modulation for each of the data directions, etc.).

[1] http://www.heise.de/security/meldung/Fatales-Sicherheitsleck-bei-Kabel-Deutschland-Vodafone-bedrohte-Millionen-Kabel-Kunden-3054052.html

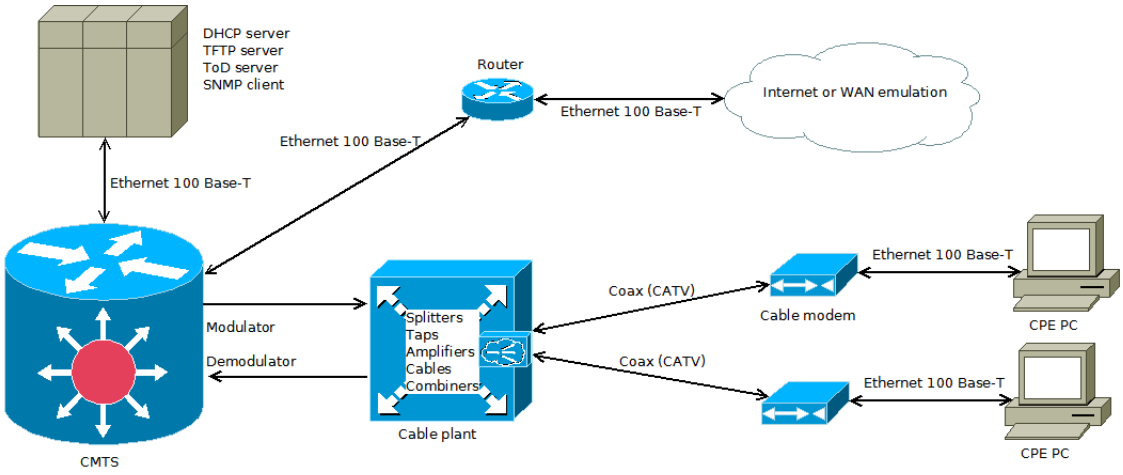


Figure 1.1.: Architecture of the lab environment

- Cable modems: Each cable modem needs a configuration file, which is transferred in the DOCSIS provisioning step using TFTP (Trivial File Transfer Protocol). These files are encoded in a special format (described in DOCSIS) and need to be properly created.
- Provisioning system: Usually the provisioning of the modems is done using an external DHCP (Dynamic Host Configuration Protocol), ToD (Time of day), TFTP (for cable modem config file) and SNMP (Simple Network Management Protocol) client for managing the cable modem parameters and other customer devices. Therefore, these system also need to be implemented. For this task, a Linux system is used and the services are offered by standard Linux daemons.
- Router: To enable connection testing of the CPE (Customer Premises Equipment) computers to the "outside" a router is required.
- CPE: A normal PC is used behind the CMs (like usually) for testing and simulating some scenarios. The connection betweend the CM and the PC is done using an ethernet connection with CAT5e cables. In the case of an embedded router (e.g. Thomson TWG870U residential gateway CM), the device acts also as a CPE device, because it does NAT (network address translation and PAT (port address translation) for several devices, e.g. up to 254 PCs with private IP address can be connected using only one public IP, which is the CPE IP of the residential gateway.

The following figure shows a simplified overview of the lab environment:

This environment is used to evaluate practical attacks against DOCSIS network. Moreover, the security features in DOCSIS and maybe some extensions (e.g. from vendors) to the protocol are being configured. To understand the implementations of the security considerations in DOCSIS some attacks are developed and executed.

This means the lab environment is starting from a very low-security point and the problems (especially security related ones) are shown. Attacks (mainly coming from the customer cable modem) are executed. The next step is to enhance the security by enabling security features built into the DOCSIS standard (at the CMTS) to reveal the countermeasures.

1.2.1.1. Lab scenarios

In this section some practical scenarios are shown. The first step is to get, with no security enabled, the environment running. This means the CPE computers can communicate with the outside/Internet. The next step is to establish more security by enabling DOCSIS security features and to try to break them by using attacks.

1.2.1.1.1. Passive attacks This part shows attacks, which are very hard to detect, because only listening on the media is done. Passive attacks already reveal a lot of interesting informations, because the following tasks can be done:

- Get MAC-addresses (and other customer related informations) of the involved devices in DOCSIS networks (e.g. CPE MAC, CM MAC)
- Decode or Decrypt the downstream traffic (payload of data packets) between CMTS and CMs

The result of those attacks can be further used to enable other attacks to work (e.g. active denial of service attacks)

1.2.1.1.2. Active attacks Active attacks are done by sending data to the CMTS, which can be detected by the provider. By the usage of a so-called diagnostic modem the following scenarios will be executed:

- Cloning a cable modem: Imitating another device and how can it be detected by the provider
- Against clients: Sending configurations from other sources (e.g., another modem)
- Unallowed service usage: Using services higher as paid for (Provisioning system attacks, bandwidth management attacks) and how to mitigate them
- Against the encryption: Are downgrade attacks possible?
- Against the authentication: Try to skip it or authenticate as a different user

1.2.2. Case study

Finally, a case study of used security related features at a DOCSIS ISPs is performed. The task is to get an understanding about which DOCSIS security functions are enabled and how they try to protect their network and the privacy. The involved work will be done passively, no attacks will be executed; based on this informations possible attacks will be listed and evaluated.

Chapter 2.

The Data Over Cable Service Interface Specification (DOCSIS)

The Data Over Cable Service Interface Specification defines methods for transporting data over a cable-TV (CATV) plant using RF (radio frequency) modulation techniques, such as QAM or QPSK to transform digital information into analog ones and vice versa [20]. The development was initiated because of the slow progress at the IEEE 802.14 Cable TV MAC and PHY working group, but some achievements got implemented into DOCSIS [57]. In fact, the DOCSIS specification succeeded because it was the first protocol implemented by most of the cable providers and vendor manufacturers. Before that, many proprietary protocols existed and those were mainly derived from ethernet. Those projects were not successful because of many problems, especially ingress (unwanted signals from the customers to the head-end). For this reason, four cable providers (TCI, Time Warner, Cox, and Comcast) in the USA formed the MCNS Holdings, L.P. in 1996 [53]. The task was to develop a specification for data transmission, without the interruption of other services used at the same coax cable plant. The result was the specification called "Data-Over-Cable Service Interface Specifications" [9]. Later on, a non-profit organization, called CableLabs, continued to work on the specifications. Moreover, the Society of Cable Telecommunications Engineers (SCTE) had the aim to do education-related work regarding the application of the DOCSIS protocol [9]. More and more standard councils accepted DOCSIS as the cable data transmission standard (e.g., ITU J.112, or ANSI/SCTE) [93]. After many positive results in real working DOCSIS environments also Europe adopted the specifications. Little changes were made to make the original standard compatible with European cable TV plants. The result is now called EuroDOCSIS and is also part of the CableLabs specifications. Moreover, the Cable Europe organization was formed to work on the European related parts of DOCSIS. Furthermore, CableLabs and Cable Europe provide a certification process to ensure the correct behavior and interoperability of different vendors of DOCSIS equipment (like cable modems or termination systems) [44] [18]. If a product passes it can be labeled "CableLabs Certified" so that people can be sure that the device will work in a DOCSIS environment, also with other vendor's products.

2.1. Topology of a CATV-system

This section gives an overview of the topology of a typical CATV-system and the associated components, which are used to enable bidirectional data transmission. Figure 2.1 shows an abstracted form of a provider architecture. The components in the left and bottom part of the image are located on the provider side, which is also called headend. The fiber and the coaxial net are the connections to the customers. The ends of the network are the attached customer devices (like TVs, Radios, cable modems), which consume the offerings from the provider. At the beginning of cable providers the network was only able to support simplex connections, therefore information was injected at the headend (see figure 2.1 TV) and the customer end devices received them (listen to the radio, watch TV). With the growth of the internet a return path had to be be constructed to enable internet access via the cable architecture. Providers had to modify their parts of the topology to make it possible for the lower frequency spectrum signals to flow back to the headend. The frequency spectrum for the information from the headend to the customers was not altered at all, so those old installations (which were only capable of Radio and TV) still worked. Many nodes in the network were replaced, like amplifiers and distributors, to support the desired frequency bands for upstream and downstream signal flow. [53]

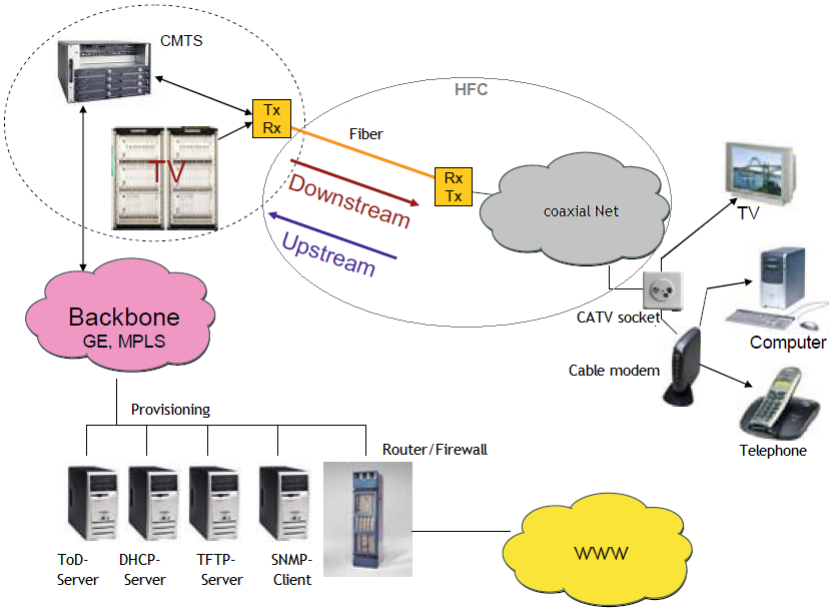


Figure 2.1.: Typical structure of a cable provider network [53]

The cable provider needs an enhanced infrastructure at the headend to offer customers the ability for accessing the internet. One important device is the CMTS (Cable Modem Termination System). The CMTS is the complement device of the cable modem (like

the automatic exchange for a telephone, or DSLAM, for a DSL connection). This device provides the MAC and PHY layer connection to the cable modem (CM) and transports data to the backbone and vice versa. The cable modem receives the information from the CMTS, which is transmitted via the cable network (Downstream) and sends it to the end device (usually called Customer Premises Equipment, e.g., a PC connected via Ethernet to the cable modem). The modem can also receive information from the CPE and send it to the CMTS (Upstream). Because of the cable network characteristics, every customer can receive all the information. The signals are present at every CATV wall socket. Therefore, different security measures s are introduced to make the connection as secure as possible. Also, other devices at the headend are needed (which can be seen in the figure 2.1 on the left side), like servers and routers. The services offered are needed by the cable modems and the cable modem termination system to operate properly. The additional services are ToD (Time of Day, used for actual time), DHCP (Dynamic Host Configuration Protocol) and TFTP (Service for simple file exchange). To do additional management of the cable modems SNMP can be used. Therefore, providers often have an SNMP management station installed at their headend to query the SNMP agents of the cable modems, e.g., for statistics about the connection. [94]

2.1.0.0.1. HFC With the emergence of the fiber technology, developers introduced a technique to use the new cables for extending the range of cable networks. Therefore, providers connected their regions with fiber cables. This is now referred to as Hybrid Fiber Coax (HFC), which describes the provider distribution cable plant. [21]

The amount of subscribers in cable networks grew rapidly, therefore a possibility to connect also faraway homes (or even cities) needed to be developed. A problem with coax cable is the physical characteristics. The attenuation is rising at higher frequencies and a connection over a long timespan is very difficult to achieve (water and ice damages the cables, or corrode connections). [53]

Moreover, it is notable that one CMTS is used for many cable modems. Usually, the same signal is passed via a tree-like structure using the HFC distribution plant to about 100 to 2000 subscribers. This value is also referred to as node capacity. One node is usually connected via a fiber cable to the headend. Typically, the size of the coax networks is going to be smaller, which has the benefit of faster speeds for the cable modems. However, this also means that the segmentation needs to be done at the headend regarding CMTS connections. At the last extent coax cables will be replaced by fiber cables, which will go directly into the homes (FTTH). [3]

2.1.1. Variations

There are differences in DOCSIS networks based on international, national or regional standards, norms or because of regulatory issues [53]. The predominantly used TV

broadcasting standard in the Europe region is PAL. Therefore, also the frequency band is arranged in 8 MHz wide channels [91]. In the US regions mainly NTSC is used. Thus, the channel frequency is 6 MHz in width [91].

Because of these fundamental differences in the frequency alignment and usage, the DOCSIS standard in Europe was renamed to EuroDOCSIS. The logical structure and the functionality are identical. For the physical layers there are differences, mainly because of the modulations used. For digital transmission of television signals ITU-T.J83 annex B is used with DOCSIS and in an EuroDOCSIS environment usually ITU-T.J83 annex A. The modulation is also slightly different, because DOCSIS additionally uses Trellis-Code for the upstream direction, whereas ITU-T.J83 is basically used for the downstream direction. Because of these reasons the symbol rate is different. EuroDOCSIS uses 6.952 Msym/s for both QAM64 and QAM256 modulation, whereas DOCSIS uses 5.056941 Msym/s with QAM64 and 5.360537 Msym/s for QAM256. Moreover, DOCSIS has several interleaver options to be configured, and EuroDOCSIS mainly has a fixed interleaver configuration. To get a usable signal out of this, the carrier-to-noise ratio highly depends on the used modulation, interleaver and frequency and power of the signal. DOCSIS modems must support a power range from -15 to +15 dBmV (QAM64/QAM256), EuroDOCSIS specify -17 to +13 dBmV with the use of QAM64 modulation and -13 to +17 dBmV for QAM256 modulation. The useable frequencies in the downstream direction for EuroDOCSIS are in the range from 112 MHz to 858 MHz (or since DOCSIS 3.0 up to 1002 MHz) with channel frequency alignment down to 250 kHz. DOCSIS has a maximum of 867 MHz specified (since DOCSIS 3.0 optionally up to 999 MHz) with a frequency plan based on HRC/IRC or STD using 6 MHz aligned frequency channel spacing. Therefore, the raw data bitrate in the downstream is higher with EuroDOCSIS (if both use the same or similar modulation schems). In the upstream direction, the frequency plan starts at 5 MHz and goes up to 42 MHz for DOCSIS and 65 MHz for EuroDOCSIS (since DOCSIS 3.0 goes up to 85 MHz for both versions). [95]

2.1.2. Security risks

The security risks occur primarily because of the physical and logical considerations of the cable network architectures. A common media is used (at least per segment/node) to transfer data and everybody can listen and read the information. This section doesn't describe the risks of the application protocols (like HTTP), it considers the issues of the cable networks at lower ISO/OSI model layers mainly. Moreover, the upper layers cannot protect its meta-data (like headers) and lower layers meta-data (like headers, management data, etc.) [61].

The following list gives an overview of potential security issues:

- Eavesdropping/Information Disclosure: Everybody can listen to the media (problem of data privacy, confidentiality, identity protection)

- Cloned modems or other devices/Spoofing: Unallowed usage of another identity or unauthorized usage of better/higher services

- Theft of service: Usage of services without payment or subscription

- Network-based attacks: Denial of Service, Man-in-the-middle attacks, Tampering: Replay-attacks

- Cable modem software updates: An attacker might load his own modified software onto the device and thus have control over it

At the start of cable networks, these risks were neglected. More and more illegal usage was detected when data services were offered. Therefore, a solution had to be developed to protect the customers and the cable operators from these risks. This was also a reason to develop a common standard. Nowadays data privacy and security is in the top three of the risks for telecommunication organizations and shouldn't be omitted from an economic point of view. [14]

2.2. DOCSIS Stack

The cable modem works technically as a bridge at ISO/OSI layer two to connect the customer network with the provider backbone. The cable modem isn't a simple bridging device, it has a lot of upper layer functionality built into it. It can be compared with a layer three switch (which has usually SNMP for management, filtering, etc.). A cable modem or cable modem termination system can act as router or as forwarding agent (like a switch). Therefore, different protocol stacks exist in the devices (they are usually connected to an Ethernet interface on the other side) to enable bi-directional IP data communication. Figure 2.2 shows the stack of a cable modem termination system (CMTS) on the left and the portion of the cable modem (CM) on the right. The components are connected using the physical media (HFC network).

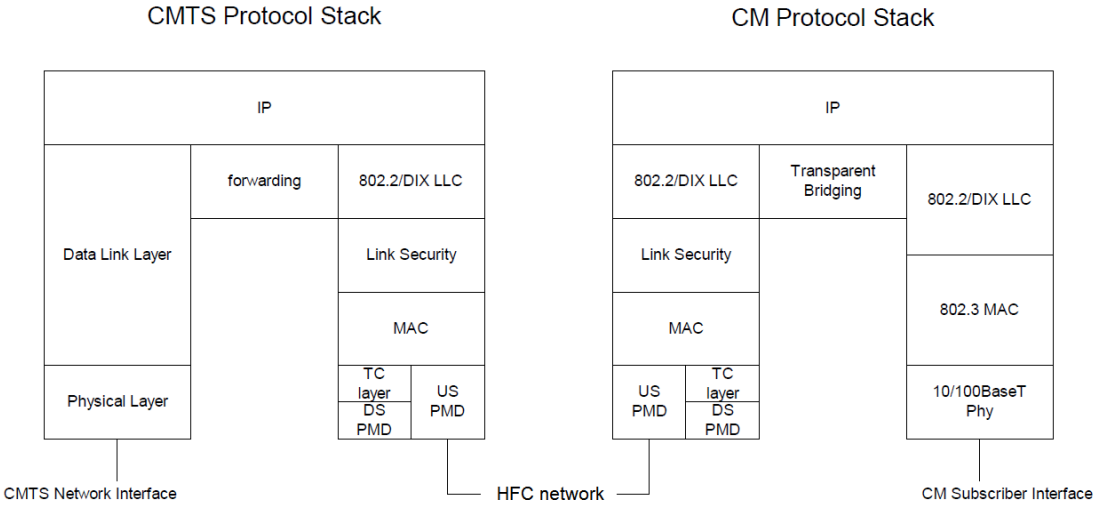


Figure 2.2.: DOCSIS-Stack of CMTS and CM [3]

The layers of the stack have the following properties and usage [3]:

- 802.2/DIX LLC: Mainly used for address resolution
- Security Layer: MAC Layer security mechanism to provide data privacy across the shared media (BPI(+)/SEC)
- MAC: Used for management messages between CMTS and CM and data exchange
- Physical layer: Used for transmission and reception of information at the physical layer (modulation, etc.), depending on the flow at the cable interface different sublayers are used (to the modem: TC layer, which is a continuous Stream of 188 byte large MPEG packets, and DS PMD sublayer, to the CMTS: US PMD), access methods are FDMA/TDMA or S-CDMA, mainly depending on the CMTS configuration (signaled to the modems via MAC messages).

For this thesis, the Link Security sublayer is the most interesting one, as it is used to implement the security measures.

2.3. The cable modem registration process

To show the DOCSIS mode of operation it is helpful to describe the cable modem registration process, which uses (nearly) all of the DOCSIS protocol layers. Figure 2.3 gives an overview of the initialization phase of a cable modem after powering up.

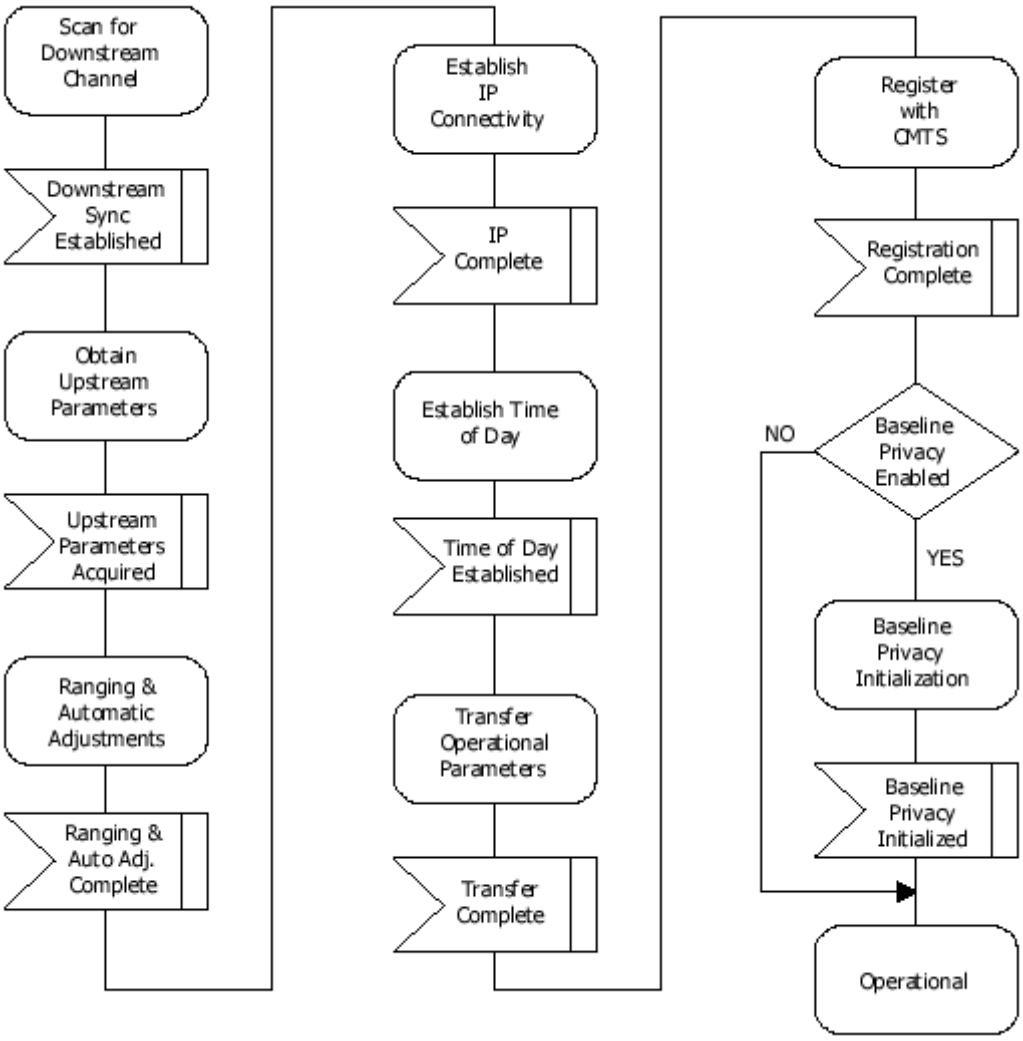


Figure 2.3.: Initialization overview of DOCSIS1.0 cable modem [89]

Downstream synchronization The first step is to search for a valid downstream channel. The tuner inside the modem tries to lock on a signal, which uses QAM-64 or QAM-256 on a given frequency. If this fails, it will try the next frequency according to the used frequency plan. The next step is to check if there is a valid MPEG2 frame (like the ones being used for watching digital TV with DVB-C tuners). This transport stream is further analyzed if its PID is set to 0x1FFE. The CMTS transmits a bunch of information repetitively: synchronization messages (SYNC), upstream channel descriptors (UCD) and bandwidth allocation maps (MAP). SYNC-Broadcasts are sent every 200msec. They are used to establish a common timing reference. If the modem detects this type of DOCSIS messages, it has usually passed Downstream synchronization. [40]

Upstream synchronization Now it looks for an Upstream Channel Descriptor (UCD), which tells the modem the upstream parameters (frequency, modulation, symbol rate, etc.). This type is usually sent every two seconds. Now the modem can initialize the upstream modulator with the received information from the UCD. To send data, the modem must wait for a MAP message, because the upstream is usually time-shared across multiple modems (TDMA). The content of a MAP message is the talk slot of a modem and the amount. Due to the fact that the CMTS doesn't know the modem, it must wait for an initial transmit opportunity in the MAP, which can be used by a new (currently synchronizing) CM to send data to the CMTS. [40]

Ranging Ranging is used to adjust the transmission parameters of the cable modem. At initial ranging the modem sends a ranging request to the CMTS. The cable modem termination system will evaluate the received information with the one stored (like comparing the timing offset, frequency response, power level, amplitude, etc.) and sends a ranging response back to the cable modem. The CM will adjust its parameters and sends it again back to the CMTS. This is done until the timing is within one microsecond, frequency within 10 Hz and power level within 0.25 dBmV. A transmission by the cable modem is made by sending a request to the CMTS, which then will respond to the request and give the CM a transmit opportunity in a MAP. The ranging process occurs at least every 30 seconds for each cable modem to also adjust to cable plant changes or other undesired effects on the HFC network and is known as station maintenance. [40]

IP connectivity The modem should now be able to communicate with the CMTS. The next step is to obtain a cable modem IP address. The method used for this is the Dynamic Host Configuration Protocol (DHCP). The modem asks for configuration parameters via a discover and request message. A DHCP server, usually connected to the CMTS at the headend, responds at least with an IP address, subnet mask, Time of Day server address, TFTP address and TFTP filename. It is also possible that another DHCP server provides more information to the modem. The modem sets its TCP/IP stack parameters to the values received and proceeds with the next step. The IP address is later used for management and addressing the cable modem from the provider headend. [99]

Time of day Reception The next step is to get a time from the Time of Day (ToD) server. This is a simple procedure, a request is sent to the time server and a response is received. The protocol used is RFC 868. The server returns a 32-bit time representing the number of seconds since 00:00 (midnight) 1 January 1900 GMT [83]. Since DOCSIS 2.0 this process is an option, but many modems still request the time via a ToD server at initialization. [99]

Transferring Operational Parameters Providers usually offer different subscription options (e.g., different speeds for home or business customers). To configure the parameters according to the contract a configuration file is used. This file is now downloaded by the cable modem from a TFTP server (the server address and filename were provided by the DHCP server). The protocol used is called Trivial File Transfer Protocol (TFTP), which is specified in RFC 1350. After a successful download, the modem verifies the file (usually using MD5), because there might be transmission errors, due to the fact that TFTP is UDP based. The CM applies the values in the configuration file (default values of the modem will be overwritten). There can be many values in the file (but only a few need to be present, like network access enabled, class of service for download/upload speeds, etc.). The configuration file can also be used to signal the modem to use a different physical downstream or upstream channel (thus the modem must reinitialize on the given frequency). Moreover, parameters for Voice-over-IP, advanced services (e.g., RIP, L2TP, static MAC address assignments), or filter rules can be set at modem level via this configuration file. The encoding of these files is Type-Length-Value. Therefore, also manufacturer dependent parameters can be easily implemented and used. [99]

Registering The cable modem sends some of its learned parameters (e.g., from the configuration file, like download/upload speeds) to the CMTS via a registration request. This step is also called transferring operational parameters back. The CMTS will check the received parameters (e.g., if they are valid and not corrupted) and responds with a registration response and tells the modem the assigned service ID (SID), which it has to use for a particular type of data traffic (which corresponds to a data traffic classification definition in the configuration file). The modem must respond with an acknowledgment, so that the CMTS has the confirmation of the CM that it has successfully received the information. [99]

Initializing Baseline Privacy An optional step is initializing baseline privacy. Its use must be defined in the configuration of the modem, otherwise it will not be enabled. The purpose is to encrypt the data across the cable network, securing the data exchange between the cable modem and cable modem termination system. Keys need to be exchanged for the operation because symmetric and asymmetric cryptography mechanisms are used. At the end of this process, security associations are established between the cable modem and the CMTS to protect the SIDs, and thus the data communication, from eavesdropping. The exact operation will be discussed later in the DOCSIS versions sections. [19]

The shown cable modem registration process is slightly altered and enhanced since DOCSIS 3.0, as it provides EAE (Early authentication and encryption) and channel bonding. After finishing the initialization sequence successfully the CM can communicate

with the CMTS to pass data traffic and is now in the operational state. Usually, the modem stores the downstream/upstream channel parameter information to shorten the initialization time at next power up. [19]

2.4. DOCSIS 1.0

This section very cursorily covers the DOCSIS 1.0 features. Furthermore, the security considerations are shown in more detail. The main goal of the first version of DOCSIS was to guarantee interoperability of vendor equipment so that a provider can choose the manufacturer for the headend and the customer equipment independently. Moreover, this makes the equipment usually cheaper and better testable. Many features of DOCSIS 1.0 are considered to be optional and therefore many components were not used. This resulted in lots of security problems (e.g., changing of parameters or even the firmware through SNMP was possible from the customer/CPE side). [30]

This list gives a quick overview of the DOCSIS 1.0 features [30]:

- QPSK and QAM modulation and thus compatibility with most of the existing cable networks (analog and digital TV signals can coexist)
- Up to 42.88 Mbit/s data throughput in downstream direction
- Up to 10.24 Mbit/s data throughput in upstream direction
- Efficient usage of upstream bandwidth using TDMA (rather than CSMA/CD, therefore fewer collisions)
- All data packets have a variable length, no usage of unneeded bandwidth
- Class of service support (to support basic parameters of Service Level Agreements, like speed considerations)
- Optional Security at MAC layer (BPI)
- Management of devices using SNMPv2
- Initial device configuration using files downloaded via TFTP from the headend

2.4.1. Baseline-Privacy-Interface

DOCSIS 1.0 also introduced a specification for security aims and mechanisms, which the involved components (CMTS, CM) must support. The specification has the primary goal to provide data privacy across the subscribers. The used method for this is cryptography with encryption of the information. For this task a key is needed. Therefore, a protocol for key exchange and agreement was developed, called Baseline Privacy Key Management. This protocol does not provide a secure authentication of cable modems or the cable modem termination system. [52]

Another issue to solve is illegal service usage with the use of cloned modems. This issue is a difficult task and was therefore skipped. Only a minimal authentication is provided using the MAC address of a cable modem. This measure is surely not enough, because the MAC address is readable by any eavesdropper, even when the content is encrypted. The reason is that the link security mechanisms are on top of the (normal) MAC layer, only the content of MAC packets and some headers can be encrypted. This method is no protection against cloned modems, which is explicitly stated in the specification. [34]

Baseline Privacy extends the MAC layer and adds one sub-layer. The underlying layer uses Service IDs (SID) for data flows. These, in turn, are comparable to quality of service data flows or VLANs with priorities. They define a type of data and are mainly used for the data scheduler of the CMTS, which allocates bandwidth for modems. At the cable modem initialization step a service ID is allocated and assigned to the modem. Because DOCSIS 1.0 only stated best effort data flows (BE) each data flow is handled equally (for data rate and burst settings). If Baseline Privacy is now turned on, the Service ID (SID) gets a Security Association (SAID). An encrypted datagram contains, beside the secured content, an extended Header (EH). This header gives information about the security mechanisms used and the related Service ID. To add the functionality of key agreement two MAC management messages got introduced: BPKM-REQ for requests regarding security keys and BPKM-RSP for responses. These messages are exchanged between cable modems (sends requests) and cable modem termination system (sends responses). The keys for data encryption also need to be re-keyed. The lifetimes of the keys are told to the modem via the BPKM protocol when the keys are issued from the CMTS. The modem itself must issue a request in time (before the expiration of the old key) for a new key. How the operation of the baseline privacy works is described in the next segment. [66]

The Baseline-Privacy-Interface (BPI) is separated into two parts. One defines the used cipher suites for encryption and decryption of data packets. Moreover, it defines the format and rules how to apply the cryptographic methods to the information. The second protocol (BPKM) is used for distributing the keying material and initiating a secure channel between modems and CMTS. A security association (SA) is used to form such a channel. During the modem registration, a primary SA can be established (if BPI is enabled in the configuration file). There also exist other types of Service IDs (e.g., for multicast data). Each of the SIDs can be equipped with a security association and thus encrypt data traffic. In the case of multicast data, a security association is shared between a single CMTS and any participant in the multicast group. To apply the cryptographic algorithm to a given SID, the SA uses traffic encryption keys, a CBC initialization vector and a cipher suite identifier (e.g., DES 40 bit, DES 56 bit). To exchange this information between CMTS and cable modems BPKM is used. It uses RSA to establish a shared secret, which is used for the key exchange. The modem issues an authorization request using BPKM, which includes the cable modem public

key (usually stored along with the corresponding private key in CM memory, RSA 768 bit or 1024 bit), an identifier (e.g., MAC address) and the SIDs to encrypt/decrypt traffic. The CMTS now generates an authorization key (using the received public key from the modem), which also includes a sequence number (used to distinguish key at rekeying/reauthorization) and the list of SIDs which the modem can be a participant of. Finally, this information is sent to the modem as a reply. The CM now issues requests for traffic encryption keys (TEKs), which are used to protect a given SID. A key encryption key (KEK) is used to protect the TEKs. DES (56 bit, ECB mode) is used by the KEKs to secure the TEK inside. The KEKs are derived from the authorization key because of the limited lifetime of a TEK. A key response of a modem also includes a key lifetime and a sequence number. Moreover, a keyed HMAC (using SHA-1) is used to authenticate keying messages. The key for this is also derived from the 160-bit long authorization key. [34]

2.5. DOCSIS 1.1

Version 1.1 of DOCSIS added a lot of functionality and tries to solve provider issues (e.g., security related ones, data flow related ones). A problem with DOCSIS 1.0 was device cloning. The new version added the functionality to detect cable modems at the registration step if they try to copy the MAC address from another legit CM. Moreover, authentication of the modems can be done using digital certificates. Most of the modems only needed a new firmware to upgrade to the new DOCSIS version. [30]

Another benefit was the introduction of different MAP creation algorithms, which are used for the allocation of the modems at the upstream. Unsolicited grant service and real-time polling service were introduced in DOCSIS 1.1 for supporting quality of service (QoS). However, a vendor can introduce its own algorithm, the specification is open for this as it will not influence the basis of the standard or the interoperability. [74]

The enhanced features are now shortly named [30]:

- MAC collision detections at the CMTS
- More enhanced security specification (BPI+, modem authentication using digital certificates)
- Optionally SNMPv3 for management (or SNMPv2, fully backward compatible)
- Voice over IP support
- Service flows (enhanced form of class of service, which was basically only a prioritized first-come-first-served-scheduling algorithm)
- Piggybacking of upstream bandwidth requests [75] (improves upstream performance, less transmit requests for upstream data)
- Fully backward compatible

2.5.1. Baseline-Privacy-Interface-Plus

The first version of BPI had no sufficient security regarding authentication of modems. The improved features are described in the following.

Certificates The authentication of modems towards the CMTS is done using digital certificates. A PKI is introduced so that the CMTS can verify a valid cable modem. A root CA (issued by CableLabs) is installed inside the CMTS. CableLabs also issues manufacturer certificates, which are used at modem production to be saved inside the devices. The CMTS checks the certificate of a modem at registration by using this chain of trust (CM certificate->Manufacturer certificate->Root CA) to ensure the authenticity of the subscriber modem. The X.509 certificate of a modem includes the MAC address and other parameters, typically the serial number, vendor and the valid period. [37]

Data and key encryption The usage of DES with 40-bit key length is marked as weak and shouldn't be used anymore. The suggestion is to use 56 bit DES for encryption of SIDs. In order to encrypt, the TEKs 3DES (EDE mode) must be used now. Therefore, the methods for deriving the key from the authorization key are altered. [37]

Authentication RSA with 1024 bit should be used (but 768 bit RSA can still be used). [37]

Key storage The implementation of the DOCSIS and BPI standard were often inadequate regarding the key storage and generation. Therefore, it is now defined to do this according to the FIPS-140-1 (security level 1) specification. The components storing the sensitive information must be production grade and the user should have no (easy) physical access to the data. Moreover, does it also state how the security modules can be embedded to the core processor and how to secure the operation of the cartographic modules (e.g. no physical test points and debug infos). Moreover, does it also state how the operating system can be secured (e.g. authentication). [90]

Secure Modem Updates Authentication of the firmware code before updating can be done now. A manufacturer or a provider can sign the update, which is then first checked if it's valid at the CM and only installed afterwards. [90]

Data flows The concept of data flows (and their classification) was vastly enhanced. Therefore, also the mapping to SAIDs and the creation of these were extended. Now the creation of dynamic (e.g., VoIP traffic at calls) and static SAIDs (at the CMTS, e.g., for multicast data flows) is supported. [82]

2.6. DOCSIS 2.0

The main purpose of the DOCSIS 2.0 standard was to offer symmetrical data speed services for the providers' customers. Therefore, additional upstream modulations (8-QAM, 32-QAM, 64-QAM) and access modes (S-CDMA) are defined. Moreover, the frequency bandwidth in the upstream direction was enhanced to support 6.4 MHz (before DOCSIS 2.0 it was 3.2 MHz bandwidth). The introduced S-CDMA (Synchronous Code Division Multiple Access) access mode and 128-QAM trellis coded modulation makes it possible that several modems (up to 128) can transmit data simultaneously on a single upstream channel, which can be accomplished by the use of a spread spectrum approach. Another benefit of S-CDMA is the ingress cancellation, which means the CMTS can work with bad signals (noise robustness). The security specification (BPI+) remained unaltered. [52]

The following list gives a brief overview over the enhanced features of DOCSIS 2.0 [52]:

- Enhanced upstream capable bandwidth (up to 30.72 Mbit/s)
- Additional upstream modulations with Trellis coding (S-CDMA, 128-QAM)
- Support for video conferences
- Fully backwards compatible

2.7. DOCSIS 3.0

In 2006 DOCSIS 3.0 got finally released. One of the biggest improvements was the possibility of channel bonding and an enhanced modem registration process. By the use of channel bonding, it is possible to use several data channels at once, thus forming a larger logical channel, which results in higher throughput. A simplified view is the parallel concatenation of many modems at different channel frequencies. Moreover, IPv6 support was specified. To reduce some attacks (like Denial of service) an ARP rate limit was defined. Because of improvements and enhancement of the modem registration process, the security specification was renamed from Baseline-Privacy-Interface-Plus (BPI+) to SEC, which is described below the feature list of DOCSIS 3.0. [32]

A quick feature list of DOCSIS 3.0 improvements [32] is given here:

- Channel bonding: Used to increase the data throughput in downstream and upstream direction
- IPv6 support (Dual-stack support, also management of cable modems)
- Early Authentication and Encryption (basically BPI+ applied in an earlier step at the cable modem initialization)

- AES 128 bit (CBC mode, 128-bit blocks) for data encryption
- Fully backwards compatible

2.7.1. SEC

The improvements and changes (compared to BPI) of SEC are the following :

Data encryption In order to enhance data privacy, it is possible to use the symmetric algorithm AES (128 bit long keys, 128-bit block size). It is stated as an option. Therefore, also DES with 40 or 56 bit can still be used. The CM tells the CMTS at initialization which cipher suites it supports. Depending on the priority list of the CMTS it decides which one to use. [41]

Authentication The RSA key used in the X.509 certificates of the modems can now be 2048 bit long. This is also suggested by introducing the new PKI. Due to backwards compatibility, also 768 bit and 1024 bit public keys are supported. [41]

Certificate revocation A mechanism for revocation of certificates is usually a component of the PKI management. A certificate is usually valid for its lifetime. It can be the case that it is not trustworthy any more. Another reason to mark a certificate as trustless is the end of a contract to a customer (who has brought his own modem). There are now two possibilities to do the annulment [41]:

- Certificate Revocation Lists (CRLs)
- Online Certificate Status Protocol (OCSP)

None of them are required and there is no central service for OCSP or informations for CRLs. How these procedures work is described in detai in RFC 3280 (CRLs) and RFC 2560 (OCSP).

Configuration settings integrity A new message integrity check (MIC), called MMH, is introduced. This algorithm can be used to check the configuration parameters at the CMTS. As with BPI+ the MMH-MAC is a keyed hash, which is used by the CMTS to validate the CM's received configuration settings and to prevent alterations of the parameters (TLV encodings). [41]

Physical protection of keys The storage and protection of keying material must be done according to FIPS 140-2. This means the device must be in an enclosure and the chips shall include standard passivation techniques to protect the information from environmental or physical damage. Moreover, some other requirements are stated, such as using production grade PCBs (Printed circuit boards). [41]

EAE In the previous version of DOCSIS, the establishment of the secure channels using BPI is done at the last stage in the modem initialization process. This is very problematic, as especially the configuration file is transmitted in clear-text. Now it is possible to initiate Baseline-Privacy at an earlier stage. This step increases the overall security enormously. Figure 2.4 shows the differences of doing normal BPI(+) and SEC with EAE enabled. The modem will be authenticated right after the ranging phase. To support EAE, the CMTS sends DOCSIS management messages (MDD) periodically to inform the cable modem that EAE is enabled and if it is mandatory to use. Now a secure channel is formed, and the MAC datagrams are secured. Therefore, when requesting an IP using DHCP, getting the time, and receiving the configuration file are encrypted, whereas normal BPI(+) does the establishment of a secure channel at the end of the modem registration phase. The feature EAE can be enabled at the CMTS on a per-MAC or per downstream channel basis. [41]

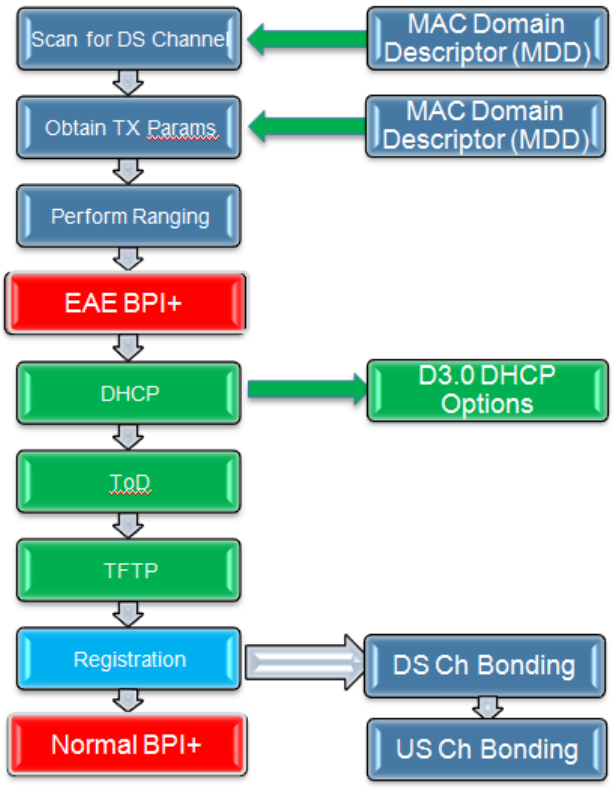


Figure 2.4.: Early Authentication and Encryption (EAE) [99]

Management messages In order to support additional physical features (like channel bonding) new management messages were introduced (e.g., REG-REQ-MP for channel bonding). To safeguard these packets, their encryption and decryption are added to the Baseline-Privacy protocol. [41]

2.8. DOCSIS 3.1

To compete with FTTH offerings, CableLabs developed DOCSIS 3.1 to support speeds of up to 10000 Mbit/s in downstream and up to 2000 Mbit/s in the upstream direction for a customer. The improvement is possible because of smaller node sizes. A node is connected using fiber to the headend, the last mile is done using traditional coax cabling and thus resulting in a very good signal at the customer (high MER/SNR), which can handle higher modulation orders. First of all the channel spectrum is increased to achieve such high data throughput. Methods for better utilizing the frequency spectrum and for error protection and recovery are used. Moreover, no single carrier is used. OFDM is used for modulation (20 kHz to 50 kHz subcarriers, bandwidth spectrum up to 192 MHz). DOCSIS 3.1 is backwards compatible, providers can still use DOCSIS 3.0 upstream channels. Therefore, no big plant changes must be made (due to the standard usage of the lower frequencies for upstream). [49]

The following items cover the major features of the new DOCSIS standard [15]:

- Frequency spectrum usage: 108 MHz to 1218 MHz (optionally up to 1794 MHz) for downstream, 5 MHz to 204 MHz for upstream
- Up to 4096-QAM in upstream and downstream (optionally 8192-QAM and 16384-QAM) direction
- Enhanced error protection and detection (LDPC, BCH)
- New certificate-based security features (firmware upgrades, additional functionality of devices)
- Improved queueing strategies to reduce jitter and latency (e.g., for VoIP calls)
- Sleep modes to reduce power consumption when the modem is in idle state
- Backwards compatible

2.9. DOCSIS over PON

Passive optical networks (PON) are new access networks to connect users to their providers, like DOCSIS over CATV networks or DSL. The main difference is the usage of optical fibers, which are capable of 10 Gbit/s symmetrical bandwidth (and more in the future) and a distance beyond 20 kilometers from the headend to the customers.

The architecture supports a point to multipoint connection. The OLT (Optical Line Terminal) sits at the headend (like a CMTS) and services up to 128 ONUs (Optical Network Units), which are comparable to modems. To connect these two together, an Optical Distribution Network (ODN) is used. It consists only of passive parts (like splitters). [68]

There are many PON standards and the following lists gives an overview [68]:

- ITU-T G: APON (ATM-based), BPON (ATM-based), GPON (Can encapsulate different protocols like ethernet, ATM, etc.)
- IEEE 802.3: EPON (Ethernet over PON)
- SCTE: RFoG (Radio Frequency over Glass)
- And many others more (e.g., XG-PON1, NG-PON2)

Each of them hasits benefits and drawbacks. EPON and GPON offer very fast speeds and offer AES 128 bit data encryption in the downstream direction. Provisioning is usually done using a (long) serial number or MAC address. Some vendors also offer the possibility of using additional measures, like certificates. GPON or EPON uses TDMA (like DOCSIS) to share the time of the upstream access bandwidth among ONUs. [68]

The PON architecture is very similar to the one of DOCSIS. The benefit of a PON is clear: it has no electrically powered parts in the HFC plant, which minimizes problems (repairing), power costs and supports higher throughput. Providers who want to migrate their network to PON can run DOCSIS over PON (at least when using EPON or GPON). The benefit is in the reuse of the headend infrastructure, like provisioning of customer equipment (modems/ONTs, CPEs), test systems and knowledge. Thus, solutions for this, called DPoE for DOCSIS over EPON, DOCSIS over GPON and DOCSIS over Glass are developed. Moreover, the PON architecture can also be used to transport normal DOCSIS and RF channels to the customer. Traditional DOCSIS hardware can be used at the headend (CMTS) and at the customer (cable modem) location. [67]

The effect by combining DOCSIS with PON is that any problems, features or properties will be inherited. Using only PON means replacing all coax cables with optical fiber and results in high costs. Therefore, coax cable or combinations with PON based on DOCSIS will be in existence for quite some time.

2.10. Alternatives and comparison to other protocols

The first Ethernet standard was based on using a coax cable. Nevertheless, the downside of the solution was that there could only be one signal present at a given time, which is called baseband transmission. In a typical cable TV environment, another approach is used, called broadband. [53]

This section gives a quick overview over available protocols, which share some commons with DOCSIS. First, some proprietary protocols got deployed. At the rising demand of a common need, the IEEE also started some working groups (like IEEE 802.14, IEEE 802.10) to develop standards. Nevertheless, the race was won by DOCSIS. It is the one protocol which is used by nearly all cable internet service providers.

Proprietary solutions Before the deployment of DOCSIS many proprietary protocols existed. Basically, each cable provider, who wanted to enable the network to support data services, used a vendor dependent approach. Many of the techniques and methods got included into the first DOCSIS specification. [30]

One protocol to be mentioned is CDLP, which was developed by Motorola. It uses basically the same physical layer as DOCSIS used later on (especially the quadrature amplitude modulations). One of the problems with this system was the poor load management and the security. [8]

Another vendor for proprietary cable TV data transmission was LANCity. The protocol was mainly adopted in DOCSIS for the MAC layer. The problem of large cable TV networks is the distribution delay, and thus ethernet does not function efficiently. Therefore LANCity basically used an ALOHA-based approach. One of the participants (modems) in the network was elected as a master, which then grants slaves (other modems) access to the data bus. The protocol was symmetrical with a throughput of up to 10 Mbit/s using QPSK modulation. [29]

IEEE 802.10 The intent of the IEEE 802.10 working group was to build security functions for local area and metropolitan area networks, which are based on IEEE 802 standards. The goal was to protect and secure the data exchange at layer 2. To mitigate the threats of a typical LAN connection-less confidentiality (including integrity and access control) mechanisms were defined. To support these specifications for encryption and decryption of the data are defined. Because of the use of keys, also a key management protocol was designed, which worked at layer 7 that could communicate with layer 2 protocols. The original data is encapsulated into a frame, according to the framework (SDE) of the working group. The protocol works in a sublayer at the LLC layer, above the MAC layer. The standard were withdrawn, but is available on request, and the working group is currently not active. [60]

IEEE 802.14 Almost simultaneously to the DOCSIS project initialization, the IEEE 802.14 workgroup started with the development of a standard for fast data communication over existing cable TV networks. The decision was to make the protocol ATM-based (DOCSIS is IP/Ethernet-based). Much detail goes into the contention algorithm used in the upstream direction, whereas DOCSIS was at that time simply best effort. There

were some thoughts for layer two security. One was to use an IEEE 802.1ae (MACsec) like approach, the other was mainly to adopt the DOCSIS BPKM (BPI) to the standard. The development was much slower, due to the iterative development, and providers quickly decided to implement and use the DOCSIS standard and the working group was liquidated. [5]

WiMAX WiMAX is a name for one of the IEEE 802.16 solutions for the last mile. It can be used by metropolitan providers to support customers, which are up to 30 miles away, with fast internet access or other data services (like VoIP, IPTV). The security of IEEE 802.16d was mainly based on DOCSIS BPI and called the key distribution protocol PKM (privacy key management). another media was used and so some weaknesses evolved. In spring 2006 the IEEE announced 802.16e, which tackled many of the issues. Digital certificates and AES-CCM are now used to secure the data exchange between the base and subscriber station (like the CMTS at DOCSIS). [1]

Chapter 3.

Practical DOCSIS networks

In this chapter, a real physical DOCSIS network is developed and built. First, the basic configuration of the involved components is shown and explained. A very minimalistic cable plant is built, which is then used to connect cable modems to the CMTS. A provisioning system is installed to offer the needed services for the DOCSIS architecture. Next, security attacks are executed to show the risks of such networks. The range is from basic passive ones (like sniffing, getting information) to active attacks (e.g., cloning, authentication, and downgrade attacks). How to mitigate or solve some of the problems will be explained. The mitigations can be treated as a guideline for building a DOCSIS headend network because this is not mentioned in the DOCSIS standard. Moreover, advanced security issues are discussed. They range from decryption attacks, injection attacks to man-in-the-middle attacks. Insider attacks and implementation issues can also be a problem, as will be shown with real examples. Some of the problems may result from legal problems and law enforcement, which will also be discussed. In the last section legacy hardware problems and device effects are stated.

3.1. Lab environment

The goal is to get the equipment up and running, CPEs should communicate with the internet (or at least the internet gateway in the headend). The lab environment is also the starting place for the attacks described later-on. Basic settings are done according to real cable provider networks and follow standard recommendations. The provisioning of subscribers (modems) is done through a dedicated server. Although some cable modem termination systems support all needed features and thus eliminate an additional server, they are not employed in real environments due to the limited configuration settings, management of cable modems and harder debugging. All IP related settings are done using version 4 of the Internet protocol.

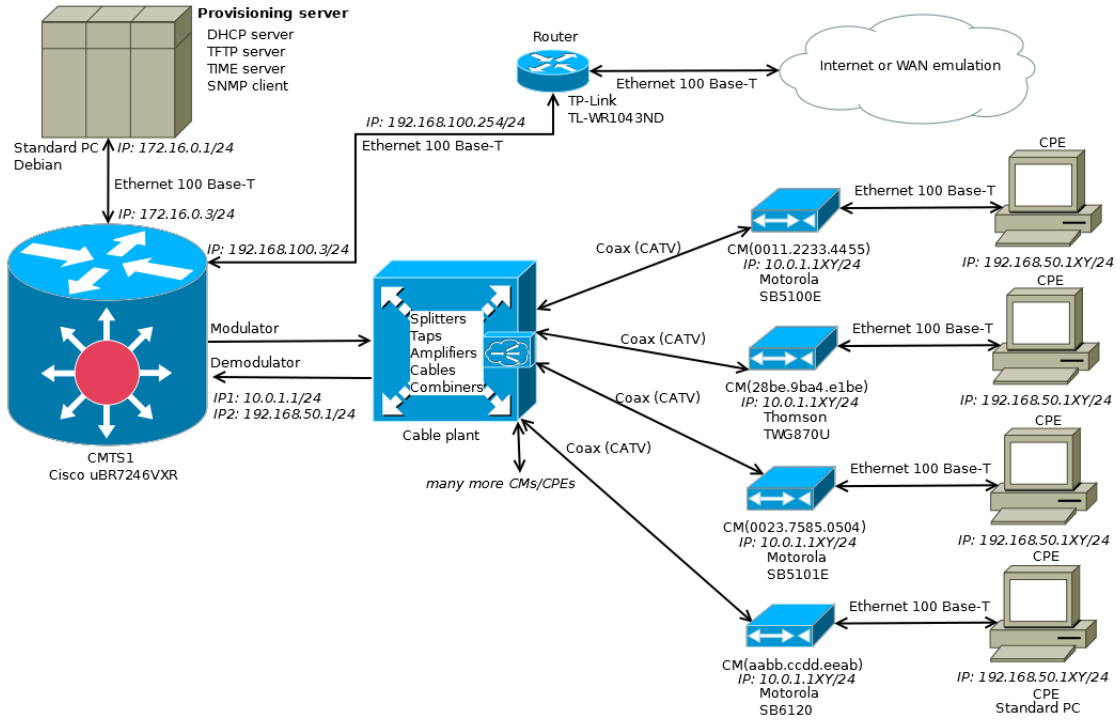


Figure 3.1.: Overview of DOCSIS lab environment

Figure 3.1 shows an overview of the DOCSIS lab. These devices and equipment will be further discussed in the next subsections.

3.1.1. Cable plant

The cable plant has the duty to deliver the downstream signals from the CMTS to the cable modems. This follows the traditional behavior of the broadcast medium. Nowadays usually all DOCSIS cable networks are two-way, therefore the upstream is also carried out via the cable plant. The signals transmitted from the cable modems must be received at the upstream inputs of the CMTS (usually at 0 dBmV reference).

Because of the RF signals used, all applicable norms must be considered, especially the CENELEC standards, like EN 60728-1 (which basically describes requirements of cable networks for broadcasting). In a real cable network analog and digital TV signals need to be protected (primarily the analog signals), otherwise the picture quality will degrade. Which outlet levels and carrier-to-noise interference are to be considered and must be met are stated in EN 60728-1. The goal is to have a signal power for a EuroDOCSIS QAM256 modulated 8 MHz channel in the range of -6 dBmV to +17 dBmV at the cable modems (with at least 31.5 dB carrier to noise ratio). Moreover, the DOCSIS physical layer specifications should also be considered (which tend to limit the power at modem

to max. +15 dBmV, and recommend max. +13 dBmV). Also, noise and EMI levels are described, the system must not transmit RF signals into air, which may cause other service interruption, like harming LTE and DVB-T signals. [98]

The RG-59 cables used have a nominal impedance of 75 Ohm and use the ISO-169-24 (often merely called "F") connector. The shielding must be at least 90 dB (Class A), usually double shielded cables are used in high power level areas. Moreover, a goal in real installations is to have a high isolation of outlets (thus they cannot harm each other), usually 10 to 20 dB. All passive components shall employ the direction coupling technique. This applies to splitters, junction boxes, and outlet sockets. Many cable providers have guidelines for (house) system installations, which also follow ITU-R Rec. BT. 470-7 (Signal norms) and EN 50083-7.

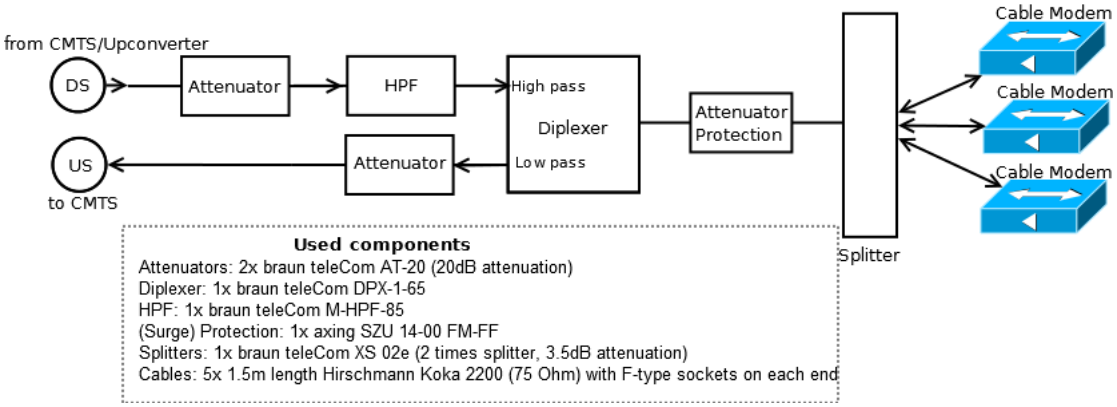


Figure 3.2.: Cable plant structure

No fiber cables or HFC structure is used in the cable plant, all cabling is done with coax cables. This should not influence any of the attack results, nor the behavior of the scenarios because they focus on upper layers of DOCSIS. Figure 3.2 shows the structure of the cable plant. The RF downstream (DS) signal is fed into the system at the left upper corner. Usually, newer cable modem termination systems already have a built-in upconverter, to adopt the IF (intermediate frequency) signal to an RF (radio frequency) signal at the chosen channel frequency. Next, an attenuator is used to lower the signal power (usually +50dBmV to +70dBmV is present after the upconverter), to reduce intermodulation and other bad behaviors of the diplexer (and other components in the signal path). The upconverter output can also be very vulnerable to incoming signals, which can destroy the output amplifier of the converter. Therefore, a HPF (high pass filter) is used to allow only the frequencies from the downstream signals to pass, the lower frequencies will be attenuated. The next stage is a diplexer. This component splits the frequency bandwidth into a lower and upper band at a defined split frequency (in the ideal case, in real some non-linearity is present). The downstream

channel signal is forwarded to the output, which basically connects to the modems. The lower frequencies, coming from the modems, are split to the lower band output of the diplexer. This signal is fed back to the CMTS upstream port. The upstream signal needs to be around 0 dBmV at receiving. To get a high SNR at the upstream port the modems need to send usually between +40 to +50dBmV, thus it needs to be reduced in overall signal power. Therefore, a 20-dB attenuator is present before and after the diplexer. Also, the unwanted parts will be attenuated at the upstream attenuator. The cable at the right side of the diplexer (which is at the end connected to the modems) carries all frequencies needed for bidirectional communication. Lower frequencies are used for upstream coming from the cable modems and higher frequencies for the downstream channel to the cable modems. Both signals (in- and outputs) of the CMTS/upconverters are sensitive to DC power. A protector is used after the diplexer to filter out all signals (including DC) below some kHz. Moreover, this component can also handle surge protection (like small strikes). A splitter is connected to this device to distribute the signal to numerous cable modems and perhaps other equipment (usually also to TV sets, radios, or set-top boxes). This device also has a directional coupler effect, the outputs have an autonomy to each other. Usually, a signal from one output to another has an attenuation of at least 20 dB. Also, normal socket outlets behave like this, to minimize erroneous impacts from one output to another. All components have F-type connectors installed, and at least RG-59 cables are used with a rating of Class A (min. 90 dB shielding) according to the CENELEC standard. The length of each of the headend cables (starting from CMTS to splitter) is max. 50cm, in order to minimize non-linearity and ingress effects.

3.1.2. CMTS

The CMTS connects the RF cable plant with the IP (or Ethernet) based network of a provider. It provides the ability to offer bi-directional IP based services, such as internet access or voice and video services. Usually, this device is placed at the headend, the RF signals are usually fed to the nodes (splits of the coax cable plant) using fiber cables. In the lab environment, the cables of the cable plant are directly connected to one downstream and to one upstream port of the CMTS. The network side interface (NSI) is used to connect to the provider core network using Ethernet. The CMTS performs the switching and routing functionality between these two interfaces. Although some older cable modem termination systems can be configured to be bridges, the used Cisco `uBR7246VXR` cannot. One drawback of this CMTS is created by the fact that if multiple cable modem termination systems are used by a provider it has to subnet the assigned IP network because it cannot assign any IP addresses of the whole big network to cable modems (or CPEs). The network must be subnetted, which can result in lots of routes and entries in the configurations of the cable modem termination systems, or implement proprietary solutions (e.g., running RIP on the cable modems or CPEs,

VPN). The good thing about a switched CMTS is smaller broadcast domains. Moreover, the connection to the provisioning system can be better secured, because in a bridged CMTS configuration the headend network is directly connected to the broadcast domain of the cable modems, or an additional switch or router has to be connected to form different broadcast domains or IP networks.

Initial configuration This section shows the steps to configure the CMTS. Only relevant and most interesting settings are shown. The complete configuration file and version info regarding the components can be found in the appendix. First, some basic configuration is done. A hostname, domain, and password are set, subnetting and classless routing is activated. Not required services, such as HTTP server and CDP, are deactivated. The IP connectivity to the provisioning server and the core router is configured as shown in listing 3.1. To manage the device remotely, SSH keys are generated, and the console is activated. Now the cable interface related settings are configured, which is shown in listing 3.2 and are described now. First, the DOCSIS type is set to EuroDOCSIS (line 1). There are no modulation specific settings done (especially in the upstream), no noise reduction or ingress cancellation parameters are optimized, the default settings are used. The downstream for channel one (line 6) is set to the frequency 443 MHz (line line 9), QAM256 (line 8) is used and annex A (line 7), because of European DOCSIS (EuroDOCSIS J.112) being in use. Moreover, the upconverter is activated (line 10). The upstream frequency of the first input port is set to 27 MHz (line 11) with TDMA (line 13) operation and using QPSK modulation with a channel width of 1.6 MHz (line 12). Because the device is basically a layer three router, the cable line-card needs an IP-addresses. A cable bundle (line 15) is used to be extendable and to also include further cable downstream and upstream ports to the broadcast domain and thus avoid subnetting. This bundle has IP address settings for the modem range (line 16) and the CPE range (line 17) of the customer equipment. Moreover, a helper address (line 18) is used to forward DHCP requests and let the CMTS act as a DHCP proxy. To get as much information as possible at the DHCP server (at the provisioning system) from a request the DHCP proxy at the CMTS inserts relay information (e.g., the interface where the request comes, in the case of a CPE request the remote agent ID and much more).

```
1 CMTS1(config)#interface GigabitEthernet0/1
2 CMTS1(config-if)#description Connection to provisioning server (172.16.0.1)
3 CMTS1(config-if)#ip address 172.16.0.3 255.255.255.0
4 CMTS1(config-if)#exit
5 CMTS1(config)#interface GigabitEthernet0/2
6 CMTS1(config-if)#description Uplink (GW 192.168.100.254)
7 CMTS1(config-if)#ip address 192.168.100.3 255.255.255.0
8 CMTS1(config-if)#exit
```

```
CMTS1(config)#ip route 0.0.0.0 0.0.0.0 192.168.100.254
```

Listing 3.1: IP configuration to headend provisioning and core network

```
cable freq-range european
ip dhcp relay information option
interface Cable3/0
 no cable packet-cache
 cable bundle 1
 cable downstream channel-id 1
 cable downstream annex A
 cable downstream modulation 256qam
 cable downstream frequency 443000000
 no cable downstream rf-shutdown
 cable upstream 0 frequency 27000000
 cable upstream 0 channel-width 1600000 1600000
 cable upstream 0 docsis-mode tdma
 no cable upstream 0 shutdown
interface Bundle1
 ip address 10.0.1.1 255.255.255.0 secondary
 ip address 192.168.50.1 255.255.255.0
 cable helper-address 172.16.0.1
```

Listing 3.2: Cable settings

In a real cable provider environment, the chosen frequencies are usually free, because they are inside the ISM frequency bands and can thus have negative impact on a big RF network. In the upstream path frequencies below about 20 MHz shouldn't be used, they tend to cause ingress problems (coming usually from power supplies and other oscillation circuits). Nevertheless, the reason for choosing this frequency in the lab is to minimize problems of violating the CENELEC or EMC standards due to potential transmissions of the RF frequencies into the air. To adjust the output power of the upconverter to the total downstream signal power budget the `cable downstream rf-power` command can be used. By using the `cable upstream power-level` setting the expected receive level at the input receiver at an upstream port can be set to perform slight optimizations.

3.1.3. Cable modems

Cable modems are used at the customer side to bridge the CPE ethernet network (usually a PC, SOHO router, etc.) to the cable network and vice versa. There are four cable modems connected to the cable plant splitter using 1.5m length class A RF cables using F-type connectors. All modems are two-way enabled, they share the same coax wire for upstream and downstream signals. Two of the modems are normal consumer grade modems, one of those is a residential gateway and thus a router (which acts like an attached CPE device). The other two are diagnostic modems, which can be used

to adjust DOCSIS related settings (like RF MAC addresses). They run basically the same software, but enable the access to the vendor settings through additional software. The configuration of the parameters can be done either via web-interface, serial console or through telnet. All modems can, to a certain extent, also be configured through SNMP, they support at least DOCSIS-MIB V2 (RFI). The standard software-based modems include valid DOCSIS certificates, which are bound to the corresponding RF MAC addresses (and other unique values). The list of used modems is as follows:

- Motorola SB5100E (DOCSIS 2.0 capable diagnostic enabled firmware)
- Motorola SB5101E (DOCSIS 2.0 capable standard software release)
- Motorola SB6120 (DOCSIS 3.0 capable diagnostic enabled firmware)
- Thomson TWG870U (DOCSIS 3.0 capable standard software release)

3.1.4. Provisioning system

The provisioning system is used to boot up the modems, it offers the needed services. In principle, any operating system or server can be used. It is also possible to make an all-in-one configuration on the Cisco CMTS, but this does not scale, and no provider should use this and it is not recommended by Cisco. It's mainly intended for debugging [46]. Therefore, the Linux based distribution Debian[1] (version Debian 4.8.4-1) was set up at a normal x86 compatible PC. This device is directly connected to the CMTS using the management interface (IP 172.16.0.3 at the CMTS). First, the system is installed and a user account, called `cablelabs`, is added. The next step is to connect the system with the CMTS provisioning interface and set up an IP at the provisioning system (`172.16.0.1`). Moreover, routes to the connected cable networks are added. They are needed to transfer IP based data to the cable modems (IP range 10.0.1.x range) and the CPE devices (IP range 192.168.50.x, e.g., PCs behind the cable modems) via the CMTS. The next part is to set up a DHCP server, a Time of Day, a TFTP server (which provides configuration files) and optionally an SNMP client (or NMS).

```
1 root@docsisserver:~# ifconfig eth1 172.16.0.1 netmask 255.255.255.0
2 root@docsisserver:~# route add -net 10.0.1.0/24 gw 172.16.0.3
3 root@docsisserver:~# route add -net 192.168.50.0/24 gw 172.16.0.3
4 root@docsisserver:~# route -n
5 Kernel-IP-Routentabelle
6 Ziel            Router          Genmask         Use Iface
7 10.0.1.0        172.16.0.3      255.255.255.0   eth1
8 172.16.0.0      0.0.0.0         255.255.255.0   eth1
9 192.168.50.0    172.16.0.3      255.255.255.0   eth1
```

Listing 3.3: Provisioning server IP configuration

[1] `https://www.debian.org`

DHCP After the cable modem ranging process, the modem tries to get an IP address via DHCP. For this task ISC-DHCPD [2] is used. Also other devices such as customer PCs, or routers, residential gateways and MTAs need IP addresses assigned using DHCP. There is a bunch of available options to differentiate between CPEs and CMs. One possibility is to define static MAC address entries. The decision is done based on the provided MAC address in the DHCP request. Another option is to use a vendor class identifier. A DOCSIS cable modem usually sends along with this option all supported features (like DOCSIS version, BPI support, etc.). The decision if it's a CPE or CM can be done with this distinction. The CMTS is the device which really knows the physically connected cable modems. This information can also be used to decide the IP range because this can be used by the DHCP agent to send the data from different source IP addresses (using the giaddr field in the DHCP message). A provider also needs a mechanism to bind a subscriber to a particular cable modem. For this task the MAC address of the modem can be used. Therefore, also the IP assignments of the different devices can be based on static MAC address entries in the DHCP server to differentiate between the CM subscribers. Listing 3.4 depicts some of the interesting configuration items of ISC-DHCPD using the static MAC address assignment approach:

```
1  subnet 10.0.1.0 netmask 255.255.255.0 {#subnet for CMs
2      range 10.0.1.10 10.0.1.254;
3      option routers 10.0.1.1;
4      default-lease-time 23200;
5      max-lease-time 86400;
6      filename "start1.cm"; #default CM DOCSIS config file
7      option bootfile-name "start1.cm"; #default CM DOCSIS config file
8      deny unknown-clients;
9  }
10 subnet 192.168.50.0 netmask 255.255.255.0 {#subnet for CPEs
11     range 192.168.50.10 192.168.50.254;
12     option routers 192.168.50.1;
13     default-lease-time 3600;
14     max-lease-time 7200;
15     allow unknown-clients;
16 }
17 host cm-subscriber1 {
18     hardware ethernet 00:24:d1:d2:77:d7;
19     filename "start2.cm";
20     option bootfile-name "start2.cm";
21 }
22 host cm-subscriber4 {
23     hardware ethernet 00:11:22:33:44:55;
24 }
```

Listing 3.4: ISC-DHCPD configuration file excerpt

[2] https://www.isc.org/downloads/dhcp/

The DHCP messages (discover, request, etc.) come form the CMTS and the task is to bind a known subscriber (e.g., `host cm-subscriber4`) with a known cable modem MAC address (in this example `00:11:22:33:44:55`) to an address in the cable modem IP range and to use a distinct configuration file (e.g., `start1.cm`) to the CM. This file is usually used to apply speed limits and other settings to the modem, according to the chosen subscription by a particular customer. Due to the statically defined cable modems the `start2.cm` filename gets assigned to MAC address `00:24:d1:d2:77:d7`, whereas the `start1.cm` file-string is used for all other modems. The `10.0.1.10-254` range is used for the cable modems, therefore only known clients (`deny unknown-clients`) are accepted. A provider usually doesn't want to manage all the MAC addresses or anything hardware dependent on the customer side. Therefore, all other clients are allowed in the `192.168.50.10-254` IP range (this is usually a public IP address). Another notable distinction is also the lease-times. A cable modem usually always gets the same IP address and is mostly always powered-on, whereas a customer PC is only running several hours a day and thus a lower lease-time is set. Another reason for lowering the times is also the limited public IPv4 space, to use only the really needed ones for the customer CPEs. There are many optional values setable, like the time offset (relatively to UTC) or (backup) gateways, encoded in the next-server option. The complete configuration (including hints and explanations) can be found in the appendix.

ToD The cable modems usually request date and time during the cable modem registration process. In the newer DOCSIS standard, it was changed to optional, but nearly all cable modems try it first through the time-of-day protocol (at least the lab CMs do). The protocol is very simple, it supplies the seconds since 1st January, 1900 GMT, 00:00:00, as 32 bit value [83]. Modems usually use the UDP version at port 37. An empty payload datagram is sent from the modem, which is received by the time server and indicates a trigger to send the 32-bit time value back to the modem [83]. The protocol does not try to account for any network delays or jitters. It is mainly used by the modems for their log entries. In Debian `xinetd` [3] can be installed and used to offer the time service. It only needs to be enabled in the configuration file (usually found at `/etc/xinet.d/time`).

TFTP The UDP-based Trivial-File-Transfer-Protocol is used to transfer the configuration files from the provisioning server to the cable modems. For this task the advanced TFTP-Server [4] version 0.7 is installed at the Debian server. The setup routine automatically creates a folder under `/srv/tftp` where the offered files can be stored. It can be used with `inetd` (or `xinetd`), but the simplest way is to define not to use it, and it can be simply run via `systemctl` as a daemon.

[3] `http://xinetd.org`
[4] `https://sourceforge.net/projects/atftp/`

Configuration files Cable modems can get various settings (e.g. downstream channel) during their existence in the network and during registration from the CMTS directly or via a configuration file from the TFTP server. At modem startup a type-length-value (TLV) encoded file is downloaded from the TFTP server, given in the DHCP offer, which offers the CM important operational settings. A TLV-setting can be again a TLV entry in the binary data and thus creating a tree-like structure. Which TLV settings can be present in the configuration file, or in a message between CMTS and CM can be found in [45] at appendix C.

To produce such files for the lab the free open-source tool docsis[5] version 0.9.6 is used. It translates textual representations of the settings into binary files and vice versa. The listing below shows a textual representation of the `start1.cm` configuration file, which is used as the start setting in the lab scenarios.

```
1  Main{NetworkAccess 1;          /* enables packet forwarding */
2    GlobalPrivacyEnable 0;       /* don't care about privacy */
3    UsServiceFlow                /* creates upstream service flow */
4    {
5      MaxRateSustained 100000;   /* limit to 100 kbit/s */
6      UsServiceFlowRef 1;        /* SF number */
7      QosParamSetType 7;         /* activates SF */
8    }
9    DsServiceFlow                /* creates downstream service flow */
10   {
11     MaxRateSustained 1000000; /* limit to 1000 kbit/s */
12     DsServiceFlowRef 2;        /* SF number */
13     QosParamSetType 7;         /* activates SF */
14   }...
15   SnmpMibObject docsDevNmAccessStatus.1 Integer 4;/* enable SNMP MIB object */
16   ...}
```

Listing 3.5: Start configuration for lab cable modems

There is a bunch of required entries. The first is to enable network access and thus enable the packet forwarding between connected CPE devices to the modem and the cable network (line1). To receive and transmit data via the network at least one service flow for upstream and one in the downstream direction must be present (line 3, 9). Moreover, some optional TLVs are set. SNMP is enabled so that modems can be managed from the provisioning SNMP client (possibly at the headend, line 15). The `start2.cm` configuration file is created analogously, the max. downstream speed is set to 2000 kbit/s (line 11) and the upstream to 200 kbit/s (line 5). To generate the binary file the command `docsis -e start1.txt keyfile.txt start1.cm` is issued. The binary data also includes a message integrity check for the cable modem (MD5 digest) and

[5] `http://docsis.sourceforge.net`

a keyed hash (MD5 HMAC, key in `keyfile.txt`) for the CMTS, which can check the correct settings of the modem at CM-registration.

Another optional encoding is a packet classifier (IP/port/MAC based), which can be used to apply different service flows to distinct PDUs (e.g., UDP VoIP traffic gets higher priority by using another prioritized service flow). Also, firewall rules are possible (e.g., block SMTP), as well as payload header suppression, CPE IP count limit, or vendor-specific options. There are hundreds of such TLVs defined in the appendix of the DOCSIS specification [45].

SNMP and Syslog An SNMP client can be used to query at agents (e.g., the cable modems). Moreover, it receives SNMP traps or notifications, which are sent by the agents. The used software is Net-SNMP [6] version 5.7.2.1. The trap daemon is activated and the authentication community `cablelab` was added to receive logging information at UDP port 162. The used SNMP version in DOCSIS is usually v1 or v2c, which is only community (password) based and has neither encryption nor secure authentication. SNMP can be used to change operational values of a modem immediately. The exact behavior and which values exist are described in the DOCSIS-MIB.

As Syslog server `rsyslog` [7] version 8.4.2 is used to receive messages from remote devices. Usually, a modem sends an entry if a link goes up (e.g., CPE is attached) or down. It is simple to configure, it merely needs to be enabled to receive remote TCP or UDP syslog entries.

The complete configuration files for the SNMP trap and `rsyslog` daemon can be found in the appendix.

3.1.5. Core router

The core router should only allow valid devices to access the internet (or other IP based services). Therefore, only a route for the IP range of the connected devices to the subscriber modems is added.

```
1 root@fw1:~# ifconfig br-cmts 192.168.100.254
2 root@fw1:~# ifconfig br-cmts | grep inet
3 inet addr:192.168.100.254  Bcast:192.168.100.255  Mask:255.255.255.0
4 root@fw1:~# route add -net 192.168.50.0/24 gw 192.168.100.3
5 root@fw1:~# route -n
6 ...
7 192.168.50.0        192.168.100.3   255.255.255.0   br-cmts
```

[6] `http://net-snmp.sourceforge.net/`
[7] `http://www.rsyslog.com`

```
8 ...
```

Listing 3.6: Core router configuration

Listing 3.6 shows the steps which need to be done at a Linux-based router. The ethernet interface used to connect to the CMTS is called `br-cmts`. Moreover, the router in the lab does NAT/PAT (it has one public IP address at the upstream port), so that the CPE IP addresses can be used to access the internet.

3.2. Attack scenarios

In this section security weaknesses of the cable network, including parts of the headend network, are described. For each of these attacks, countermeasures are shown or described. The vulnerabilities mostly result from an incorrect threat model, which was only improved in newer DOCSIS standards. Providers thought by enabling bi-directional data transmission the model would not change, but this assumption was wrong and led to massive security flaws [2].

3.2.1. Passive attacks

This section describes security issues, which can be exploited without sending data. A provider cannot detect such attacks, nor is an internet subscription by the unit a must. Usually, all signals are present at all cable outlet sockets (at least at a node). From the attack perspective, it can be compared to war-driving (detecting vulnerable Wi-Fi networks). However, the big difference is the surface. A cable network is much bigger compared to the Wi-Fi network range and the attacker is harder to detect, because any socket outlet, splitter output, or tap output can connect to a potential malicious eavesdropper. If the shielding of the RF components is not done well, then it might also be possible that the signal can be intercepted over distances several centimeters or even meters [31]. Due to the nature of cable networks, each device in a node receives the same signals from the headend. This section covers how sniffing can be done in the downstream (upstream sniffing is evaluated in chapter 4) and how to enable DOCSIS data privacy to mitigate the risk of decrypting the data.

3.2.1.1. Sniffing downstream

This section covers the options of getting the raw DOCSIS data out of the analog signals and how to find the parameters of the signal. First of all, hardware is needed to demodulate the RF-signals. The chosen device needs to be attached to the cable network using a splitter or tap. If the signal cannot be split, because the power of the

outlet is too low (e.g., when connecting a bunch of devices to one socket outlet) a cheap RF amplifier (drop amp) can be used.

The available options for demodulators are (not restricted):

- Cable modem in promiscuous mode
- SDR (software defined radio)
- TV-Demodulator (QAM256/QAM64)
- DSP (perhaps programmable analogous to an FPGA, with ADC)
- DVB-C or ATSC card

Some old cable modems allowed the use of a non-DOCSIS compliant mode to switch the MAC filter basically off. The result is having all received frames at the CPE side of the cable modem, acting the modem in a promiscuous mode. [58]

Another possibility is to use a software defined radio (SDR). They are more or less modulator or demodulators to interface RF signals, which can be controlled by software. Also, the costs are relatively low and can be easily obtained. The downside of the cheaper SDRs are the modulator bandwidths, because most of them can not capture the relatively broad signal (ca. 8 MHz) of a common DOCSIS downstream signal. Therefore, the cheap RealTek RTL2832U[8] with Elonics E4000 tuner devices can not be used.

Due to the DOCSIS modulation, a normal TV-Demodulator can, in theory, be used to get the digital data. Although this modulator needs some interface and, depending on the circuitry some control, which makes it very expensive. However, hardware designs of cable modems may help if developing your own hardware solution. The same is true for a digital signal processor (DSP) solution, which might use an ADC or in turn a demodulator. The easiest way is to use a DVB-C card, which usually uses the same frequencies as the DOCSIS downstream signals. The card is used to watch digital TV channels at a PC and the received signals are usually 64-QAM or 256-QAM, therefore perfectly capable of DOCSIS information reception.

The lab uses EuroDOCSIS, therefore a DVB-C card is used, which has a USB interface for the PC side. The used *Astrometa USB DVB-T/T2/C + FM + DAB*[9] stick uses a RealTek RTL2832P IC as demodulator and host interface, a Panasonic MN88472 frontend (also demodulator for DVB-C) and the Rafael Micro R828D tuner.

[8] http://www.realtek.com.tw/products/productsView.aspx?Langid=1&PFid=35&Level=4&Conn=3&ProdID=257

[9] http://www.astrometa.com.tw/integrated_en.html

Countermeasures The main reason for the easy sniffing attacks is the usually non-existent physical protection of the cable sockets and the usage of standards (like modulation and MPEG stream). A basic mitigation would be to apply seals to connected devices, which are made by an authorized cable technician. It is clear that this is not practicable if a new device needs to be connected, removed or exchanged because the provider or a dealer needs to be called or informed. Moreover, this would result in high costs. Another idea is to reduce the needed RF power level at the socket and SNR. This can be tuned to be at the minimum, so no splitter or amplifier can be attached to connect more devices to one socket. In theory this works, but in practical networks it does not because of natural variations mainly due to cable temperature dependency. A more practical way, which was at least done by some providers, is band filters. They block exactly the DOCSIS frequencies, if no modem is attached to a particular cable or the subscriber has no cable subscription. Although it seems a good idea, it needs a technician and provides only basic protection. Often the filters were removed from the customers because sometimes the TV channel frequencies and also the DOCSIS channel frequencies might be changed by a provider from time to time [30]. For an eavesdropper, the newer DOCSIS standards (since 3.0) makes it harder to extract useful information out of the captured signals, if channel bonding is enabled. The reason is the simultaneous usage of several physical RF channels. Therefore, an attacker needs to capture all those channels, which logically form a bigger DOCSIS channel. Channel bonding cannot be seen as a countermeasure anymore because capture hardware is relatively cheap (ca. 100 to 25 Euros per channel) and an optimized processing software to reassemble the data is available.

3.2.1.2. Decoding DOCSIS downstream traffic

This section extends sniffing attacks with the software part and thus decoding the digital signals to get useful information. The first step is to scan the frequency band and to try to acquire a lock on a particular frequency with a distinct (de)modulation scheme (64-QAM or 256-QAM). If there is a lock, the received data needs to be checked if it is a valid MPEG transport stream containing the DOCSIS identifier `0x1FFE`.

A cable modem might be used to determine the frequencies and modulation schemes, but if a carrier is found the modem needs to be immediately turned off, otherwise it will try to communicate with the CMTS and thus be detectable by the provider. There is an easy solution for this, an upstream band blocker. With this simple RF band filter, no communication with the CMTS can be done.

To do the scanning and decoding of the lab DOCSIS downstream channel, an Ubuntu 16.10 x64 based PC is used. Details about the sniffing and decoding hardware setup can be found in the case study chapter 5. For scanning the frequencies the tool `w_scan`[10]

[10] `https://linuxtv.org/wiki/index.php/W_scan`

or `dvbscan`[11] can be used. If a suspicious channel is detected, it can be tuned to using `dvbtune` (using the found frequency, symbol rate and PID, usually 0x1FFE), which is part of the `dvb-tools`[12]. To get the DOCSIS data `dvbsnoop`[13] can be used. It can be used to save, view or debug the data stream.

Another solution is the program `packet-o-matic`[14]. The new `ng` version comes with a bunch of plugins. One plugin is intended for scanning for DOCSIS channels, it is configurable (timeouts, modulations to test, frontends to use) and can automatically add the found channels with its parameters to the input stream section of the program. It can process many packets from a bunch of sources, due to its multi-threaded and modular architecture. A DOCSIS input can then be started using the specified frontend and pom-ng automatically processes the data stream. An output can be added to dump or save the assembled DOCSIS PDUs. This can be done in the form of an Ethernet interface, which can be monitored and captured from other programs (like Wireshark or tcpdump), or pcap files (also separated into flows). Moreover, it supports events. Those can be fired at the parsing state of the protocol analysis. Actions can be performed if some patterns or communications are found (e.g., save detected MAC addresses, VoIP calls, HTTP sessions including graphics). It also has an API for connection tracking, extending it to support new protocols is very easy. Moreover, payload analysis is also possible (e.g., gzip archives or multiparts in protocols). [64]

Countermeasures An obvious mitigation is to use cryptography to encrypt the data between CMTS and cable modems. This can be accomplished by enabling privacy in the configuration files at the provisioning system. Therefore, the value of `GlobalPrivacyEnable` is changed to `1`. After regenerating the cable modem configurations, the modems need to be reset or rebooted (which can be done either via SNMP, the CMTS (removal from the station maintenance list and thus they need to register again), or manual re-powering. One problem with this solution is that privacy is not mandatory and the modem can also select one out of a bunch of cipher-suites. Therefore, a modem can freely choose if it enables the BPI(+) functionality or not. Therefore, on the CMTS the `cable privacy`-command accepts the option mandatory and the priority of the cipher suites should be set accordingly. One issue with this is, that it is not possible to turn off very insecure ciphers (e.g., DES 40 bit) at the lab CMTS. Moreover, a modem is also allowed to send a self-signed certificate. If only trustworthy modems should be allowed, then this makes no real sense. Because a malicious user can simply create his own certificate and therefore successfully pass all security checks.

[11] `https://www.linuxtv.org/wiki/index.php/Dvbscan`
[12] `https://sourceforge.net/projects/dvbtools/`
[13] `http://dvbsnoop.sourceforge.net/`
[14] `http://www.packet-o-matic.org`

3.2.2. Active attacks

This section deals with basic threats of active security attacks and their mitigations in the DOCSIS lab network. The results of such attacks are a major problem for the providers, which lose billions of US dollars due to theft-of-service in cable networks [69]. The detection of malicious activities is also important for providers, at least to minimize the impact or the range of an attack. Legit modems from paying customers might work only limited or not anymore, because of attacks described in this section. Modification of modems or other components (also software) is getting easier, due to the darknet and other online retailers, which offer comprehensive prices for hacked modems. How the vulnerabilities can be exploited will be shown at the scenarios. The attacks range from impersonating (modem cloning) to illegal SLA improvements (e.g., more bandwidth speed than paid for).

3.2.2.1. Cloning modems

Cloning is the form of impersonating someone else's cable modem. There are many reasons why somebody wants to do this. It can be for troubleshooting, e.g., if a customer has problems then the technicians don't need to fetch the device from the customer. Of course, a malicious user is often interested in cloning someone's modem. The intention might be to get the service level of the genuine subscriber or to do illegal activities with the usage of the cloned identity. Depending on the clone level, measures to hinder those attacks are shown. The problem with all of these is the design of the specification and its implementations. First basic clones are described. More enhanced clones (which also includes the certificates for authentication) are evaluated. Finally, an attack scenario is shown and executed in the lab and the countermeasures are shown.

3.2.2.1.1. MAC cloning

The first distinction to be made here is if the provider uses several MAC domains or only one. If the clone and the genuine modem are online in the same MAC domain, then it is not possible to do a long-time communication with both CMs online. If the subscriber and the malicious modem register at different MAC domains, probably at different frequencies or if the modems are located in different nodes, then there might be a chance that each of them can communicate and have a valid registration. This situation is shown in figure 3.3. The reason why this may work is to be found in the behavior of a typical provider architecture. Two CMs work in different broadcast domains (like two separate VLANs at a switch), therefore the MAC addresses are in different logical topologies. The provisioning server is usually connected to all of the CMTS and therefore doesn't care which CMTS or line-card (DOCSIS port) the modem is connected to. In this case, MAC trading comes into the game. If there is one common provisioning system, which knows the desired paid customers and therefore

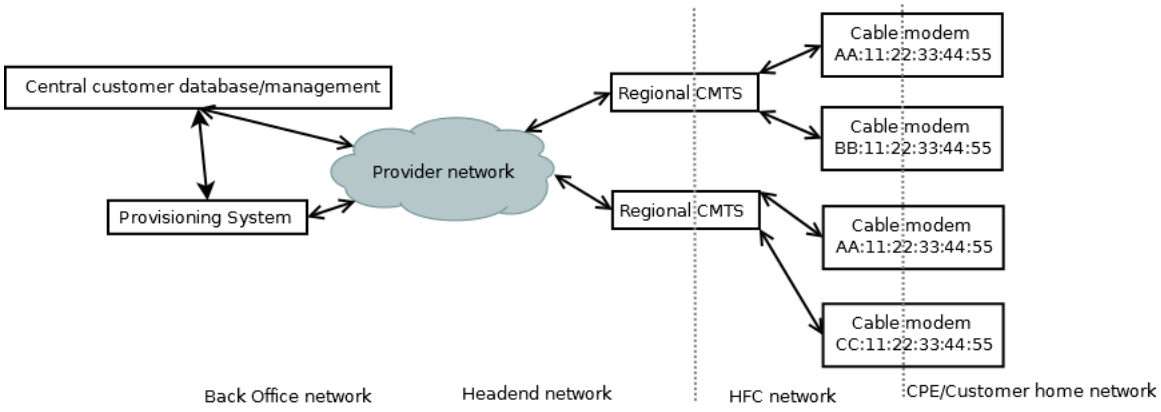


Figure 3.3.: Typical provider network

the cable modem MAC addresses, then a modem with the particular MAC can be registered at each DOCSIS MAC domain. Providers often use a central management of their customers, therefore the provisioning system is also often centrally located (e.g., connected via the backbone to the CMTS using VLANs or MPLS) [30]. Of course, this configuration only works if routed CMTS are in use (like the lab one), which need distinct IP ranges for the DOCSIS line-cards (and their outputs or MAC domains).

Basic clones Cloning involves mostly copying and using someone else's MAC address of the user's cable modem RF interface. There are basically two steps for this to accomplish. First, the MAC address must be obtained and the second is to apply and use it at the malicious modem. The signals in a DOCSIS network are broadcasted. Therefore, each subscriber gets the same information (at least in the same HFC node) from the headend (downstream direction). The DOCSIS PDUs do have the MAC address in it, and they can be extracted from the signal, whether privacy is turned on (payload is encrypted) or not. This can be done easily, as already described in the passive attacks section or as seen in the case study (chapter 5). In this way potential neighbors for cloning can be obtained.

Moreover, a hacker can also listen for modems which try to register at the cable modem termination system. The assigned CM configuration file (according to subscription), DHCP requests and therefore also the possible attached CPE MAC addresses can be determined (in the case that EAE is not enabled or used), using passive sniffing approaches. The benefit for a malicious person is that for a CM MAC address the according IP is known (even if BPI+ is enabled). The hacker can now (usually) check if the IP is in use (using a normal subscription modem) by the legitimate modem. If it is not, he can go online with the sniffed MAC, and it does not harm the other (offline) CM.

In case of a denial of service attack, a rogue modem can be put to a DOCSIS socket with the targets MAC address set at the RF interface. The CM will try to register and (at least on the same DOCSIS MAC domain) thus kick the regular modem offline because it will have a ranging timeout (or wrong ranging information due to the rogue CM messages).

To use the information (at least a valid CM MAC address) physical hardware is needed. Providers and manufacturers do sometimes need analyzers or diagnostic modems to troubleshoot issues or implementations. Of course, this hardware is not intended for malicious persons, but it can also be used in a rogue way. DOCSIS protocol analyzers are available from various vendors, and many of them also support emulating a DOCSIS modem (mostly DOCSIS 1.1 or 2.0), therefore also the MAC address can be set. One big downside is the very high costs of such analyzers. A cheaper solution is offered by some modem manufacturers (like Motorola), in the form of special diagnostic modems. As the name suggests, their intend is to offer diagnostic features, like detailed information of the operation status or also setting different parameters of the unit (at least RF MAC address). The software of these modems is basically a modified version of normal customer grade modems. Their purpose is also troubleshooting, e.g., to emulate a customer modem at the headend (with the subscriber RF MAC set to it). However, it has to be stated that most manufacturers only sell the modems to big providers to mitigate the risks that they will be used as rogue modems. Nevertheless, some websites sell them (or copies) [30]. Some manufacturers shipped unfinished software with their regular customer modems, so-called shell based modems [69]. The vendor did not disable the shell (not at startup nor at normal use). Therefore the modem can somehow be controlled by the end-user. Of course, this software is interesting for malicious persons to manipulate the intended behavior of the device (e.g., set RF MAC address). Another approach is to reverse engineer the software (and hardware parts) of a normal modem and develop your own firmware for it, to additionally support all needed features. Of course, also self-developed hardware (based on DSPSs, or SDRs) can be used, if it supports the physical requirements for DOCSIS (e.g., QAM modulation schemes).

Moreover, it has to be stated that, according to the DOCSIS standard, a regular customer is not allowed to alter settings of the CM. Therefore, each described solution is not a valid DOCSIS cable modem (at least not DOCSIS certified). [34]

Semi-perfect clones Basic clones can be detected because of their behavior and supported features (e.g., no BPI+ enabled nor do they have valid certificates or other identifiers such as serial numbers). More enhanced copies also have valid certificates (according to the PKI based on the root CA of CableLabs) and parameters like the regular CM. Of course, to get the according certificates is the hardest part as they are stored in a (hopefully) secure way in the regular modem. In the cable modem registration process, some features of the modem are also sent to the CMTS and the

DHCP server. The feature-set of the clone needs to be (at least) the same, and it also needs to send the exact information as the original modem. Therefore, the information needs to be sniffed or obtained in a more enhanced way (e.g., by using SNMP attacks to dump the information from the original modem). Of course, if physical access is given to the regular modem, then it is easier to obtain this information. For example, the memory can be dumped in a few seconds from the regular modem, and the data can be extracted out of the dump (if they are not encrypted or packed in some vendor specific way).

It is very hard for a provider to detect semi-perfect clones, the best way for a provider is to check the validity of the cable modem certificates. Of course, this involves all the issues of a PKI. One security issue with this infrastructure has just occurred. A manufacturer had forgotten the private manufacturer certificate in its software and therefore your own valid cable modem certificates can be signed with it [15]. This is a serious problem and it seems that malicious persons already used it to sign their own, self-generated cable modem certificates [16]. To mitigate this issue providers need to black-list the compromised vendor certificates.

Perfect clones The biggest problem for a provider are perfect clones. The behavior is exactly like the the one of an original modem, and also the software is the same. Although this seems hard to achieve, it is actually very easy if physical access to the device is available. Due to the lack of physical security requirements inside the case, it is easy to access the data memory. Most manufacturers use some type of flash ICs, usually NAND types, which don't have security features (such as read-out protection) [30]. Therefore, with the usage of an appropriate programmer it is possible to extract the flash memory content. This dumped data can now be programmed to a similar unit. Therefore, the same hardware, including revision, must be used to run the software.

Another approach is to use the bootloader of a CM. Some of them support reading the memory at distinct addresses or write the data to a TFTP server. In the past, some devices got dumped through a wrong update process in which the boot process stops at the bootloader. Another idea is to test for undocumented SNMP commands (e.g., boot to NULL and perhaps the boot process halts at the bootloader) or interrupt the boot in another way (e.g., shorting pins). [30]

Another method is to find software vulnerabilities to dump the memory somehow. Of course, this approach is very specific and involves knowledge of a particular device (e.g., architecture, used software, etc.).

[15] https://www.heise.de/security/meldung/AVM-entweicht-geheimer-FritzBox-Schluessel-3463752.html

[16] https://www.heise.de/security/meldung/Entfleuchter-FritzBox-Schluessel-zum-Ausstellen-falscher-Zertifikate-missbraucht-3465065.html

Attack scenario To simulate a cloning attack the MAC address of a modem is copied to a diagnostic modem. Of course, only one modem can be online at a particular time. If the regular modem is not online, the clone is able to register and CPE devices can communicate, like on the normal modem. If the legitimate subscriber modem is now connected to the same MAC domain, it tries to register at the CMTS. The first step is to synchronize in the downstream and to obtain the parameters, which will work normally. However, when it tries to adjust its transmission parameters (in the ranging procedure), the CMTS will reset the status of the rogue modem and thinks that the modem is re-synchronizing and thus the initial ranging is done. The results are T3 timeouts at the rogue modem, which correspond to ranging issues. The normal subscriber modem sometimes could finalize the ranging, but because of the rogue modem, which also does the periodic ranging, it gets timeouts. Therefore, the CM resets and reboots. The regular lab CM was only sometimes able to register, and a communication was only possible for a few seconds (typically below 5 seconds). Because of the reboot time, registration and ranging timeouts the rogue modem can communicate longer (at least some seconds, typically 30 seconds or more).

Of course, a modem can also ignore periodic ranging (there will be T4 timeouts, so the modem will reset anyway, but it might be longer online), but usually a DOCSIS CMTS will reset the modem state, if it does not respond and will also apply the suggested changes to the ranging messages from the CMTS.

Countermeasures For minimizing the problem of sniffing CM, RF MAC addresses only smaller networks (node sizes) help, but it is still possible to capture the signals and decode it to get the MAC addresses in the segment of the eavesdropper. Also, EAE helps in this case. It made the sniffing of additional modem related parameters (e.g, capabilities in the DHCP discover message) and attached CPE devices harder (e.g., DHCP discover, therefore CPE MACs and associated IPs), due to the encrypted transmission of this data. The usage of sniffed addresses is another big issue, mostly addressed by the manufacturers, because they have usually a consecutive MAC address range. The CMs do not have any physical protection, and thus it is easy to copy or alter the software of the devices. Vendors should apply protection mechanisms, or at least use better grade flash chips with read-out protection features. At least the DOCSIS certificates and production-related parameters, like serial and MAC addresses should be placed onto a ROM. Moreover, the usage of one-time programmable flash would help, so that the reprogramming of the flashes with sensitive content is not possible (e.g., RF MAC, certificate). Of course, in such situations the normal firmware (application memory) should be placed at re-programmable memory to support updates of the software. Another very good approach can be accomplished by the DOCSIS SoC semiconductor producers, which can embed some small amount of permanent storage (possible to be one-time programmable) for sensitive modem data. Another approach could also be to outsource the security parts, e.g. into a SIM card, which handles the

cryptographic parts of the architecture (only store certificates, serial number, MAC, or may also do encryption). Although this would not help for already sold diagnostic and shell based modems, it would prevent hackers from using normal customer grade modems as clones. On the other hand, providers should verify the architecture and implementation of the modems, especially for the CMs and in the best case before buying in the mass for the customers. Many attacks are possible due to software issues in the CM's firmware and insecure hardware decisions.

For example, it does not make sense that a modem can register anywhere in the provider network (e.g., the customer modem is located in New York, but he can still attach his modem in San Francisco).

At least the following steps could be performed to render it harder for attackers to carry out a successful cloning attack:

- Bind CM to specific MAC domain or DS/US port(s): Some providers use multiple MAC domains on one customer node (e.g., old DOCSIS 1.0 CMTS for legacy modems, D3.0 CMTS for newer modems). If a D3.0 modem tries to register at the old CMTS, it gets a configuration, which tells the modem to switch to the frequency of the newer CMTS. Still, this is already problematic, the modem registration will not be encrypted, and sniffing is easily possible for an eavesdropper, and it is very likely that this RF MAC can then be used by a malicious person on the old CMTS. Therefore the modem should get no response (no DHCP, nor TFTP and no ranging) when trying to do the registration at the old CMTS, which forms another MAC domain at the same node. Moreover, a customer modem may be assigned to a specific downstream and upstream port of the CMTS. Maybe the provider network shares the MAC domain in several node segments, but distinct downstream and upstream ports are connected to the specific nodes, then the MAC domain approach will not be enough. Although load sharing would not work properly (at least the automatic ones supported by Cisco), it will decrease the probability of usable RF MAC addresses for an attacker. Of course, this approach is vendor dependent, and it will involve a special architecture of the provisioning system.
- Network traffic filtering: Block DHCP reply messages (e.g., offers, ACKs, etc.) from cable interfaces at the CMTS (mitigation also works for clones). Moreover, by filtering only valid DHCP messages, it is also not possible to run your own DHCP server at the customer side to provide IP addresses for another subscriber CMs and their connected CPE devices.
- Enable BPI+ and EAE: Although the encryption does not help directly to solve the cloning problem, the enhanced authentication of BPI+ including certificates does. Moreover, if the CMTS supports EAE it is highly recommended to enable this feature, as an eavesdropper cannot capture the CPE MACs (DHCP, etc.) at

the cable modem registration process. If the whole plant uses only valid DOCSIS 3.0 modems, then it can be configured to be mandatory. If only a really small amount of older CMs are used, then the CMTS vendor might support a hotlist, which defines excluded modems from the EAE feature, which includes those legacy CMs.

- Proprietary cloning detection algorithms: Some of the vendors (e.g., Cisco, Arris) offer their own solutions for detecting malicious activities, like modems which are registering very often or at different CMTS ports. At least the solution by Cisco reports cable modems, which register at different ports of the CMTS. In the lab scenario, the feature reported only detected clones if the clone and the genuine modem were at different DOCSIS ports and if the ports were configured in different domains (different node). Of course, the features can help for simple cloning attacks and report problems. But one big drawback of the features is the support for only local cloning attacks at a particular CMTS, not to detect clones in the whole provider network (which usually consists of many cable modem termination systems).

To conclude the attack it has to be stated that the attack vector, its range and the countermeasures mainly depend on the provider architecture (mostly its distribution system, e.g., HFC nodes) and the used provisioning system behavior. The best mitigations of cloning attacks for a provider is an intelligent provisioning system, which checks the state of ranging and registering modems. It should check if the CMTS and the according DOCSIS line-card port-state for a CM is meaningful. Moreover, it should check if the registration steps are done in a valid way (e.g., cloned modems might download the TFTP file many times, because it is one of the last steps during registration and the normal modem may also try to do ranging and thus the connection of the clone might be disrupted). Moreover, periodically checking the registered modems and comparing them to the database (e.g., if subscriber modem is online at the right CMTS and port) should be done, based on the CMTS information. Although SNMP messages can be easily manipulated (because usually v1 or v2c is used), it is a good idea to also periodically get information out of the modem SNMP agents and compare them to the subscriber database (e.g., user A with RF MAC X got a CM model Y from vendor Z with a particular hardware and software version).

3.2.2.2. Bypassing settings

This section describes several possibilities of using configuration files from other undesired sources, which are not intended by the provider. The technique is also referred to as bypassing configuration [30]. Depending on the headend network of the ISP and the cable modems, several methods are available to choose the actually applied configuration

file for the CM. The following list gives a brief overview over the most relevant scenarios to execute a chosen configuration file attack:

- From customer side connected device (e.g., a connected PC runs a TFTP server with the desired configuration)
- From another ISP source (e.g., other TFTP server in the headend of the provider or another filename), or upload (overwrite) own file
- From local memory (e.g., use pre-stored file in the memory of the cable modem, perhaps also manufacturer default configuration when shipping the modem)
- Via diagnostic or shell-based modem (insert the file directly, e.g., by copy and paste, using the console of the modem to use its own configuration)

The first distinction of which attack might be successful is to determine the modem type. If it is a CM which can be controlled by the user (e.g., diagnostic, shell-based, etc.) then there are plenty of possibilities to alter the cable modem registration process and therefore also the used configuration file.

Although DOCSIS states that a cable modem should have no user input from the customer and only the provider should be able to control the modem, some CMs violate this rule. Depending on the features of a diagnostic type modem it is very often possible to alter the TFTP IP, which is told to the CM upon the cable modem registration process in the DHCP offer. This type of modem usually also has the option to specify a custom filename and overwrite the one received in the DHCP message. Moreover, it is also handy to use a local stored one, which might be useful for cable plant technicians, so they can test a particular (maybe created on the fly) configuration file, without the need to alter the configuration of the provisioning system (e.g., the stored configurations at the TFTP server). On the other hand, those features are very problematic if they are in the wrong hands. A malicious person can force to load a different configuration file and may violate provider rules.

Analogous to diagnostic modems there exist shell-based modems. They are normally not intended for technical analysis, it is rather the manufacturers have forgotten to disable the console in- and outputs of the device. Thus, a user can control the device according to the supported feature-set (commands, etc.). Some of the newer modems run a Linux-based OS and very often they are based on the TI (now Intel) Puma SDK. In this case, the Linux-shell offers plenty of functionality; the cable modem registration process can be controlled by the user. Another mass of CMs run an eCos-based operating system, mainly the Broadcom based SoCs. In general, this OS is also open-source, and it can be downloaded from the manufacturer website [17].

Another possibility is to exploit vulnerabilities in the customer modem. Usually, the interface to the CPE devices (e.g., the ethernet port of the CM) is up when the device

[17] http://ecos.sourceware.org/

is powered on. The TCP/IP-Stack is usually also initialized at the boot-up. Therefore, communication to the modem from the CPE side is usually possible. A webserver at the CM tells state and statistics, which might also be handy if the RF link is not working. This behavior is usually independent from the RF interface state. Moreover, a CM learns MAC addresses upon boot, and it does not alter or delete them (until it is rebooted). Therefore, a connected CPE PC can ping the device rapidly so that the CM learns the MAC and its IP-address association fast. If the CPE IP is now set to the one of the TFTP, then there is a chance that the modem will contact the CPE device and try to download the TFTP file from the CPE device. This attack is also known as ARP spoofing or ARP poisoning. The technique can also be used to perform a man-in-the-middle attack between the CM and the TFTP server to capture the original configuration file. It works on some modems because they do not distinguish between RF and CPE interface, the interfaces are all in a bridge, and therefore it is irrelevant on which physical interface which IP or MAC address can be found. The vulnerable modems are – at the moment - Motorola SB2100, SB3100 and the SB4100 [30]. It also works on some early SB5100 builds, but nowadays this issue is fixed in newer firmware versions.

The whole headend network for the cable modem registration process needs to be securely configured. Also, the TFTP server is a crucial part. TFTP also provides the ability to write files to the server using the protocol. If the service at the headend is not properly configured, it might be possible to write configuration files to the configuration file server. If this is possible, it is very likely that this configuration files can be used by a CM and thus they might be accepted by the CMTS, if the CMTS shared-secret for configuration files is not set to mandatory.

Attack scenario A typical attack is to load a different configuration file from the cable provider TFTP server. Moreover, this attack involves an already valid registered CM but might be easily extended to also use a different MAC address and thus someone else's CM (very dependent on the provisioning system and CMTS). If a correct filename is known, then the attack is very likely to succeed, because even if a shared secret is configured the file will be valid, as it is intentionally put on the TFTP server by the provider (maybe for other customers or devices). One of the problems which might arise are device specific settings inside the configuration file, like vendor specific SNMP settings, or static IPs and VoIP settings. Of course, those issues depend on the TLV parameters in the CM configuration file.

The attacker needs a user-controlled modem, like a diagnostic or shell-based CM. The more difficult step is to get valid filenames. There are many possibilities to get this information:

- Social engineering: (e.g., talk to users on the cable network to check their RF parameters and ask for configuration filename)

- Sniffing: If EAE is not enabled the configuration files (including the filename in the DHCP offer and the TFTP packets) can be sniffed, even if BPI+ is enabled.
- Guessing: Some provisioning systems use a conventional naming scheme. The name might be related to a customer (e.g., customer ID), to the modem (serial number, or MAC address), or is simply an incremented number. Maybe it is also the name of an offered service (e.g., `speed_100_5.cm`).
- SNMP: The downloaded configuration filename can be queried from the SNMP agents of the CMs. Depending on the firewall, filters of the modem and security settings of SNMP (e.g., the well-known keyword public is used for reads) it might be possible to access another CMs SNMP agent. In this case, there will also be some more vulnerabilities, and it is very easy for an attacker to get to nearly all configuration filenames, by simply queering the other modems (which typically use continuous IP addresses).
- Brute-forcing: If none of the above methods succeed there is always the possibility to try brute-forcing all possible filenames. Of course, this task is very likely to have a long duration. To increase the probability of a valid configuration file a word-list might be useful, so that common names are first tried. Moreover, it will look very suspicious for a cable provider if there are many tries on the TFTP server to get different filenames (especially if they are from one source IP address).

If the intended configuration filename is now known, the attacker set its CM device to use the specified name and resets the modem to perform the cable modem registration process again. The modem will now ignore the string in the DHCP offer which defines the filename and overwrites this with the statically set name. In the next step, the chosen file is downloaded and applied to the modem.

The concrete lab scenario is now further described. The Motorola SB6120 diagnostic modem (MAC 00:11:22:33:44:55) is configured to use another filename. As the chosen configuration does not include any specific settings for a particular modem or vendor, the diagnostic modem has no difficulties or problems in applying it.

Countermeasures As with most of the attacks, the provisioning system is a very crucial part in the DOCSIS environment. The TFTP server should only allow files to be read. Moreover, it makes sense that the service is only available inside the cable plant of the CM IP addresses and not publicly available via the internet or the connected CPE devices. Therefore, it makes sense to apply a firewall between CMTS and provisioning system or use built-in firewall features of the CMTS to permit only valid CMs to reach the TFTP server (and maybe also other provisioning services, like DHCP, SNMP, Time, etc.).

To make it harder for an attacker to guess or determine the configuration filename, dynamic naming methods can be used. Of course, this possibility must be supported

by the provisioning software, but it can dramatically increase the security. When the DHCP server forms the DHCP offer, which contains the TFTP filename, it must tell the TFTP server (or another service/script, etc.) to generate and serve the appropriate file for the particular CM. Moreover, access to the file needs to be done one time only, when the CM downloads the configuration as part of the registration step. The file can now be deleted or removed from RAM. If a malicious user tries to download the same file (the name might be sniffed), it will get no answer (or no useful data) from the TFTP server, because the file is not present anymore. Apart from this feature, also dynamic firewall rules might be used. Only CMs during the registration process need access to the TFTP, TIME and perhaps also DHCP (CPE devices usually also discover for IPs, after successful CM registration) services and thus only at this point of time need IP connectivity to those services. The firewall will only pass traffic from the CM to the provisioning system at the cable modem registration process, which can be determined from the CMTS.

Regular monitoring the CMs might also help in identifying malicious users which load different configurations. One possibility is to query all modems for their configuration filename (the DOCSIS-MIB defines a distinct OID for this). The returned value of a CM can be checked against the intended configuration filename and if it doesn't match alterations were done and further investigation can be started. Beside the filename, also the settings can be queried by the modems and checked if they are the intended ones (e.g., using the customer database which determines the selected subscription). Although this idea sounds good, SNMP replies can be easily faked by a malicious modem. Usually, SNMPv2c is used, which only has unencrypted data transmission and hardly any authentication. Some CMTS vendors also provide the ability to view the configuration filename and some of the CM parameters. Of course, this source is more trustworthy and should be selected, if possible. If more than one CMTS is used then this might not be as easy as like with one, because they should be merged together (e.g., a customer might be present at some CMTS or some line-cards, very much depending on the hardware cable plant), so that a particular CM cannot be present at many CMTS (e.g., due to an attacker who cloned the MAC address).

A malicious modem might load a configuration file from the local memory of the CM. Therefore, no TFTP session will pass the CMTS. Normally, the modem will perfectly go online, even if the configuration is loaded from another source (under the assumption valid shared-secret, configuration, etc.). The vendor Cisco included a feature in its cable modem termination systems to force a TFTP session between a registering CM and a TFTP server. This feature is called tftp-enforce. Another issue might be diagnostic or shell-based modems, when their TFTP IP is altered. They will not load the configuration via the usual TFTP server and thus fail the tftp-enforce feature. Of course, also if the TFTP file will be loaded from a CPE device, or rather via the RF interface, no TFTP data will be transmitted over the CMTS. In all of the above cases, the feature will increase the security a little bit and will make it harder for a malicious person to load a

configuration from another source. Newer diagnostic modems typically download the intended configuration told in the DHCP offer, replace it later on and thus bypass these security improvement.

3.2.2.3. Unallowed service usage

This section describes potential issues of a DOCSIS network which allows a malicious person to gain higher services than paid for and therefore to improve the subscription. Often the term uncapping is used for such attacks. It is usually associated with gaining higher speeds (than the CM subscription intends), better service quality (less delay, higher priority), or more services (e.g., IPTV services, managing built-in components of a CM, e.g., WiFi) [30].

Most of the attacks rely on a weak provisioning system, as it is the instance which has deep impact in the initialization of a CM and thus enabling services for a particular subscriber. Depending on the attack vector there are several countermeasures against typical vulnerabilities. The listing below depicts the most common methods which are used to apply customer restrictions and therefore may also offer vulnerabilities for an attacker, who circumvents those limitations.

- Authentication of modems: Impersonating someone else and therefore using another subscription. As described in the attack scenarios above, there are basically MAC clones and other cable modem cloning attacks. Besides the use of another MAC address at the modem, it is very likely that the appropriate configuration file will be loaded from the TFTP server, which was told to the CM from the DHCP server. If the attack is successful, the malicious modem will have the same subscription services as the genuine CM.
- Configuration file: The most common way to change the subscription limitations is to alter the configuration of a modem. The first step is to find a way to change which configuration is applied. Therefore, the methods described in the above attack about the usage of another configuration file might be used to choose another configuration file, instead of the intended one. One of the first vulnerabilities in early DOCSIS systems was the alteration of this configuration files because there was no check at the CMTS if the settings of the modem were the intended ones by the operator. [30] The configuration uses TLV entries to describe the settings and can be easily decoded. An attacker might modify the content, apply it at the modem and might also send the changed parameters to the CMTS. To prevent this attack, a CMTS message integrity check, which is, in fact, a keyed hash over the settings, can be used.
- Settings of CM and CMTS via SNMP: To manage the modems remotely (queering for power levels, setting WiFi parameters, etc.) also SNMP can be used. Unfortunately, a hacker might also use it to alter the settings of the CM. The goal for a

malicious person is to gain write access control to the MIB of the device to control it. Moreover, DOCSIS also specifies a big MIB for the CMTS. Some providers also use this functionality to remotely control the CMTS (at least to check SNR levels at upstreams, etc.). The mentioned CMTS SNMP access behaves analogous to the vulnerability of the SNMP access settings of the CM, as it also offers many possibilities for an intruder to gain higher bandwidth by setting the appropriate service flow to higher bandwidths or by changing other parameters of the system to get a better subscription than paid for.

- CM firmware: The firmware of the modem might also have different features depending on the firmware revision running. A provider might use the update mechanism of DOCSIS to increase the functionality of a particular modem (e.g., to enable VoIP or IPTV features depending on the subscription). Therefore, it is interesting for a malicious person to load a different software onto the device. Generally, DOCSIS offers two possibilities to do firmware updates. The first is to specify an update server IP and filename in the configuration file, the second via SNMP. The CM tries to retrieve the file and might install it. Usually, there is also a certificate check of the newly downloaded and possibly signed software. Of course, there is a version check before installing the firmware. This test can also be altered using the certificates and therefore can also be controlled by a provider to switch between firmware revisions. Nevertheless, the hardware security of the devices is generally bad. Therefore, it might be possible to copy the content of one CM to another with a flash memory programmer. [7]

- Firewall: Besides the restrictions at the CMTS and CM level also a firewall (behind the CMTS, better inside a modular CMTS) might be used to set the appropriate limits to their respective subscriptions. Therefore, also this restriction might be a target to attack. A provider might also use a firewall and not the restrictions provided by DOCSIS to introduce bandwidth limitations and other restrictions. In this case, it is very likely that the default SNMP credentials might work and unlimited bandwidth capability on the RF link is assigned to the CM (the DOCSIS configuration file does not state a max. sustained rate for the default service flow). Of course, this is not a good idea, because an attacker will have a good chance to control the CM and the traffic on the DOCSIS network (e.g. using the VoIP service flow for regular traffic, which has high priority).

Attack scenario Most providers use the configuration file to apply a distinct service level to a subscriber modem. In order to change the subscription a malicious person changes the content of the configuration. In this scenario, a configuration file will be created and applied to a diagnostic CM with the features of unlimited speed and highest priority for the data flows with up to 254 CPE MAC addresses.

The first step is to create a new configuration with the desired parameters. The text representation of the file is stated below:

```
Main
{ NetworkAccess 1;            /* enables packet forwarding */
  GlobalPrivacyEnable 0;      /* don't care about privacy */
  MaxCPE 254;                 /* allow upto 254 CPE MACs */
  UsServiceFlow    {          /* creates an upstream service flow */
    /*MaxRateSustained 0;*/   /* undlimited bandwith */
    UsServiceFlowRef 1;       /* SF number */
    QosParamSetType 7;        /* activates SF */
    TrafficPriority 7;   }    /* set priority to highest */
  DsServiceFlow    {          /* creates an downstream service flow */
    /*MaxRateSustained 0;*/   /* undlimited bandwith  */
    DsServiceFlowRef 2;       /* SF number */
    QosParamSetType 7;        /* activates SF */
    TrafficPriority 7;   }}   /* set priority to highest */
```

Listing 3.7: CM configuration file with unlimited subscription

Now the binary TLV encoded file can be created with the command `docsis -e scenariounallowedservice.txt keyfile.txt scenariounallowedservice.cm` and put onto the TFTP server.

The next step is to load this configuration file at the CM. The possibilities to do this are stated in the attack described above in this chapter. In this scenario the file is simply loaded onto the diagnostic modem with the RF MAC `00:11:22:33:44:55` and is selected to be used when powering up the device. The listing below shows that the attack succeeded, after re-powering the CM. The `MaxSusRate` is set to zero, which means unlimited bandwidth. Moreover, the `Prio` is set to 7, which means that all data traffic (because there is only one service-flow in each direction) is scheduled to best effort (`Sched Type BE`, because no scheduling type was set in the configuration) with the highest priority.

```
CMTS1#show cable modem 10.0.1.15 service-flow
MAC Address    IP Address      Host          MAC           Prim  Primary    DS
                               Interface     State         Sid   Downstream RfId
0011.2233.4455 10.0.1.15       C3/0/U0       online        715   C3/0       16

Sfid  Dir Curr  Sid   Sched  Prio MaxSusRate  MaxBrst     MinRsvRate  Throughput
          State       Type
2591  US  act   715   BE     7    0           3044        0           73
2592  DS  act   N/A   BE     7    0           3044        0           0
```

Listing 3.8: CMTS service-flows after loading the malicious configuration

Of course, this situation isn't acceptable for a provider, each connected and provisioned CM may load an altered configuration. Therefore, CableLabs and CMTS vendors developed mechanisms to avoid such attacks, which will be stated below.

Countermeasures DOCSIS offers the possibility to use a secret between the CMTS and the configuration file creator. If this secret is held secure, it may offer increased security, because self-created files (sent from a compromised CM with the unknown secret) will not be accepted by the CMTS, if the CMTS is configured to use this feature mandatory. The configuration file contains two hash-sums at the end. One is the keyed hash for the CMTS (which was created using the secret) called CMTS-MIC. This message integrity check is used by the CMTS to verify the correct and unaltered settings for the CMTS (which are a bunch of TLVs from the CM configuration, e.g., max. sustained rate). The second hash is for the CM and is called CM-MIC. It is used to verify the integrity of the TLVs inside the configuration and therefore used to check correctly transferred data without errors (due to the usage of UDP in TFTP). The used algorithm is MD5 [41]. Although a hash-algorithm called MMH (Multilinear Modular Hash) got introduced with DOCSIS 3.0, most providers don't use it and the free open-source configuration file editor `docsis` doesn't support it.

To configure the shared-secret, the configuration files need to be re-created, so that they contain the key-based CMTS-MIC. The tool `docsis` simply accepts a key-file which contains the secret. Moreover, the CMTS also needs to be configured to check the CMTS-MIC and must be set to the exactly same secret as being used by the configuration creation tool. In the case of a Cisco CMTS, the shared key needs to be set at each of the (main) cable interfaces with the command `cable shared-secret SECRET`. After re-powering the CMs, the CM with the altered configuration is not allowed to get online (`reject(m)`), due to the wrong key in the altered configuration. This can be seen below:

```
1 CMTS1(config)#do show cable modem
2 MAC Address    IP Address     I/F           MAC           Prim RxPwr  Timing Num
3                                             State         Sid  (dBmv) Offset CPE
4 0011.2233.4455 10.0.1.15      C3/0/U0       reject(m)     719  0.00   372    0
5 0024.d1d2.77d7 10.0.1.16      C3/0/U0       online        717  0.00   585    1
6 ...
```

Listing 3.9: CMTS rejects malicious CM with altered configuration

Due to the fact that MD5 is used as hash algorithm, it might be possible to brute-force the used key (or other methods). Attacks against it might better succeed because the content can also be altered with TLVs and padding, which is completely valid especially due to the feature of encoding proprietary settings (which can be arbitrary long and may contain everything representable in hex format).

Moreover, Cisco offers the ability to dynamically create a configuration file with a random secret. If the function is enabled on the CMTS, it performs several steps in the provisioning process of a modem. The first is to check if the provisioning server sends a DHCP response (which contains the TFTP IP and filename) to the CM. It sets the content of the TFTP IP to the one of the CMTS DOCSIS interface (where the CM is connected to). Now the CMTS downloads the original configuration file from the TFTP server. If the shared-secret functionality is used, then the check is now performed. If the file is valid, it generates a random secret (which is only valid one time), which is now inserted into the original filename (the optional shared-secret is exchanged) and the file is renamed to a random string (which was the CM already told at the DHCP response). This file can now be downloaded by the CM from the CMTS (which acts as a TFTP server now). To make the usage only possible once, it deletes the configuration afterwards. If the modem registers again, it will do the same procedure, intercepting the DHCP offer, altering the configuration, setting a random name and shared-secret for the CMTS-MIC. Therefore, the configuration file cannot be re-used by a malicious person. An attacker may load his own file from another TFTP server (or from local memory), but it has to pass the CMTS-MIC check, which is in the case of this feature, a random secret (which is unknown to the attacker) and thus most theft attacks will not work anymore. [48]

Another feature by Cisco is TFTP enforcement. The CMTS performs a check if a registering CM has downloaded the configuration file over the CMTS. If the CM does not download a configuration file over the CMTS (and thus from the provisioning TFTP server), it cannot successfully register. This feature has the goal to avoid loading configuration files from local memory (or from other CPE side TFTPs). This may increase the security, but with only this feature activated it is still possible to load a different file from the provisioning TFTP server. Moreover, a malicious modem can simply first download the legitimate configuration file and afterwards replace it with another one. [48]

Very analogous to the above-mentioned security feature at the Cisco CMTS, CableLabs improved the provisioning process in DOCSIS 3.0. The TFTP server IP can be hidden, which holds the configuration files for the CMs. The CMTS has to act as a TFTP proxy, and thus the CMs communicate only with the CMTS IP because it also has to set its IP in the DHCP messages for the CMs (`siaddr` field). Like in the Cisco feature, the CMTS downloads the original configuration from the TFTP provisioning server and therefore acts like a regular TFTP client. For the modems, it acts as a TFTP server, so that the modems can download the file directly from the CMTS. It must not cache any configuration files. Moreover, the CMTS has to learn the configuration filenames (which are inside the provisioning DHCP server messages), and a CM must use this filename when downloading the configuration file from the CMTS TFTP. Another improvement is the configuration file learning feature. When the TFTP proxy feature is enabled, the CMTS has to learn the content of a configuration file and must ensure that a registering

CM gets the same settings as the CMTS has learned. The CMTS can simply check the parameters of the file and those the CM sends in its registration, and it may decide on the CMTS-MIC. Moreover, it is again worth mentioning that with DOCSIS 3.0 EAE got deployed, which enables the encryption of all provisioning data (DHCP, TFTP, etc.) and ensures that the CM is authenticated before sensitive data is exchanged. Moreover, all the features mentioned in this countermeasures section can be turned off and most of them are in this deactive state when powering on a fresh CMTS. [41]

A very handy feature to hinder IP address theft is source address verification (SAV). Since a DOCSIS network basically represents a normal ethernet network, people can simply set static IPs to their CPE devices (or CMs). A big problem might be duplicate configured IPs, or MAC addresses (on different nodes). Another issue might be unauthorized statically assigned IPs and other layer three misconfigurations. Due to the fact that the CMTS learns the IPs from the DHCP messages during the CM provisioning process, it has a database for its legitimate addresses. A CM may send data via the upstream to the CMTS and in general (if the CM is provisioned) the CMTS will forward the data to its destination. By the help of the knowledge where the data comes from (incoming US interface on the CMTS, SID of a particular modem with its source MAC), the CMTS can check if the source address corresponds to the legitimate one in its database, which has been created during the registration of the CM. The CMTS does not only learn the DHCP addresses, it also learns the statically configured ones, which are stated in the configuration file. Thus, the CMTS can ensure that only provisioned sources can send correct addresses and therefore cannot imitate any other source address. If the CMTS sees an unknown source IP, it may also issue a DHCP lease-query, to check if the IP was assigned to a particular device, but the CMTS has forgotten the entry (maybe due to a reboot, or configuration reload). [41]

Limit connected CPE devices Another problem is the cable modem CPE side interface (CMCI), which is usually an ethernet port. A standard internet subscription usually offers one public IP address to the customer's CPE equipment (e.g., a connected PC or router at the CM). Therefore, most providers want to limit the connected CPE devices at the CM to the according value. DOCSIS supports limiting the amount of MAC addresses which have access to the RF DOCSIS interface of the CM. This value can be set via TLV 18 at the configuration file of the modem [42]. If it is reset, or a value of zero is set, a default value of 1 is used. The modem first seen MAC address at the CPE modem link is saved to the modems persistent MAC table (until to a reset of the CM). If the max. specified CPE count is reached, additional MAC addresses will not be learned, and traffic from them will be discarded, and no data bridging to the RF interface will be done for the additional address.

Another possibility is to also specify the CPE MAC addresses statically in the configuration file. For this purpose TLV type 14 is being used. If one of those set MAC addresses

is seen by the CM, it will prefer those CPEs, instead of other MAC addresses (until the max. CPE MAC address limit is reached). The drawback in a real environment is the knowledge of the CPE MAC addresses of a customer device at the time of CM configuration file creation. This means that the provider needs to know the exact MACs of the connected devices at a particular customer and therefore an additional management effort has to be done to accomplish this security enhancement. [42]

It is also possible to specify the amount of usable IP addresses behind a CM at a particular point of time. It uses TLV type 35. If this TLV is set, the CM performs IP address filtering. The cable modem will learn the IP addresses and forward them if the maximum amount of different IP addresses is not reached, otherwise the packets will be discarded. The table with the learned IP addresses has no aging, the CM must be reset (re-booted) or cleared via the appropriate entries via SNMP (`docsSubMgtCpeControlReset`) to clear the list and thus set the count to zero. Moreover, the IP addresses can also be listed inside the configuration file. For this purpose TLV type 36 is being used. Because it can have multiple IP addresses, the length is a multiple of 4 and the IP addresses are stated in consecutive order. It has to be noted that the above TLVs are used for IP version 4 addresses, the same behavior can be found for IP version 6 addresses (TLV 63 for max CPE IPv6 addresses, TLV type 67 for IPv6 list). [42]

Moreover, there are options to limit the connected devices at the Cisco CMTS. The cable modem termination system offers the ability to control the maximum amount of CPE MAC addresses. This feature comes in three variations:

- Allow only a specified amount of MAC addresses at a particular modem: `cable modem max-hosts`
- Specify the maximum number of hosts for all CMs (at a DOCSIS interface of the CMTS): `cable max-hosts`
- Set the number of allowed CPE MACs globally (for each CM, at any DOCSIS interface of the CMTS): `cable modem max-cpe`

The CMTS learns the CPE MAC addresses when it first receives a data PDU containing it (from a CM). The CMTS will continuously record the number and will also record which CPE MAC addresses belong to a particular modem (or SID). If the number of MAC addresses exceeds a configured level, it will drop traffic coming from MAC addresses which are not in the list of CPE MACs (and thus exceeding a limit). [11]

Of course, such measurements can be easily circumvented by an attacker with the usage of a NAT router.

3.2.2.4. Downgrade attacks

This segment describes possible attacks aiming to minimize applied security measures. The attacks can be split into the category of encryption and authentication mechanism downgrades. Often downgrade attacks originate from protocols which offer choices. This is also the case for DOCSIS. The security measures evolved over the years and several versions are public. Therefore, different capabilities of the used CMTS and the modems deployed as well as the features used must be negotiated between the CMTS and the cable modems. The first agreement is done when a cable modem registers at the CMTS. The CM sends its capabilities to the termination system in the upstream path (registration request). Depending on these features the CMTS decides on the options (e.g., Privacy/BPI support) and sends a registration response back to the CM.

A malicious person can send an altered registration request to the CMTS with the MAC set to the genuine one (the attacked CM) and some features, such as privacy, disabled. The CMTS may now send a response back with the desired options taken by the attacker. Neither the CMTS nor the CM will now try to establish a security association, because of the disabled BPI feature. Of course, this attack will not work if EAE is enabled, but it must be set to mandatory. Otherwise, a CM is allowed to skip EAE, which thus results in a successful attack.

Until EAE is enabled and set to mandatory (and thus only DOCSIS3.0+ modems are able to connect) the authentication using certificates and the establishment of an encrypted connection can be done using BPI+. This process can be skipped by the CM. If the cable modem simply does not send a BPKM request, no encrypted channel will be built, nor will the modem get authenticated using digital certificates. Of course, an attacker may only control his own CM to skip this process, but if he can control another modem somehow, the attack might also work from remote. An attacker might additionally use implementation issues to control someone else's modem, or inject noise into the upstream and thus destroy the sent data from a genuine modem.

In general, the whole protocol has security issues, because most of the DOCSIS and BPI(+) management messages are not authenticated, encrypted or checked. Therefore, other types of attacks (e.g., denial-of-service) are possible. [55]

Attack scenario One of the scenarios already mentioned is the skipping of the BPI feature, even if the CM and CMTS supports it. Of course, the CM must be prepared to do so, and thus the scenario uses a diagnostic modem, which supports this feature to disable initiating BPI (after the usual CM registration with the CMTS). The typical lab environment is used to execute the attack, the CMTS is configured to support BPI(+), which is very common. The privacy features are not set to mandatory. Otherwise, the attack will fail. This configuration is very common because there are a lot of older DOCSIS 1.x and 2.0 modems (and manageable amplifiers) out in the field, which do

not support enhanced security measures, such as EAE. When the malicious modem (MAC 0011.2233.4455) is connected to the cable plant and powered up it will do the usual steps in its registration process: synchronizing, getting downstream and upstream parameters, ranging, getting IP, configuration and time. The configuration file will now state that the modem should enable BPI(+), or it might be implicitly given (due to DOCSIS management messages). The diagnostic modem will skip this and thus be online without BPI(+) enabled. All data transmission will be unencrypted, and the CM is not authenticated using digital certificates.

```
1  Main
2  { NetworkAccess 1;            /* enables packet forwarding */
3    GlobalPrivacyEnable 1;      /* privacy feature BPI(+) is turned on */
4    UsServiceFlow               /* creates an upstream service flow */
5    { UsServiceFlowRef 1;       /* SF number */
6      QosParamSetType 7;        /* activates SF */
7    }
8    DsServiceFlow               /* creates an downstream service flow */
9    { DsServiceFlowRef 2;       /* SF number */
10     QosParamSetType 7;        /* activates SF */
11   }
12 ...
```

Listing 3.10: CM config excerpt (Privacy enabled)

Listing 3.10 shows the desired configuration for the diagnostic modem (which is offered by the TFTP server). It has encryption enabled globally (line 2), and the CMTS has also determined that this CM is capable of BPI(+), which it has received from the CM's registration request. Depending on the diagnostic modem, there might be many ways to achieve the goal of the downgrade attack. One solution is to try loading an altered configuration file. This might not work because of the shared secret feature or other measures (e.g., checking the intended configuration from the CM at the CMTS). In this scenario, the diagnostic modem is configured to disable the start of the BPI(+) process, after it has finished the basic registration with the CMTS. Therefore, it is indifferent to the used configuration file. The CM is now fully operational and can communicate like a usual modem on the network, but its data is not encrypted nor is it securely authenticated (only with the CM MAC) at the CMTS. Figure 3.4 shows the valid online diagnostic modem at the CMTS. Of course, the other modems will show that they had a TEK key assigned to them (displayed as "`online(pt)`") and the diagnostic modem is nearby listed as online, and it is allowed to pass traffic on the cable network.

Of course, this attack works because of the BPI(+) feature set to enabled, but not mandatory at the CMTS. If it is now set to be obligatory, the CM must perform it. Otherwise, the intended access to communicate at the network will not be allowed. This was also tested in the lab environment. The only change is to enter an additional command to make privacy compulsory: `cable privacy mandatory`, which must be

```
CMTS1#show cable modem
                                                                          D
MAC Address    IP Address     I/F          MAC            Prim RxPwr  Timing Num I
                                           State          Sid  (dBmv) Offset CPE P
aabb.ccdd.eeab 10.0.1.19      C3/0/U0      online(pt)     5    !-1.50 593    0   N
0024.d1d2.77d7 10.0.1.16      C3/0/U0      online(pt)     6     0.00  592    1   N
0018.c01d.90a2 10.0.1.11      C3/0/U0      online(pt)     7    !-1.00 583    0   N
0011.2233.4455 10.0.1.15      C3/0/U0      online         8    !1.00  251    0   N
```

Figure 3.4.: List of cable modems at CMTS

entered at each of the primary cable interfaces. With only this command set, the CMs are still allowed to skip the authentication using digital certificates and therefore a downgrade to BPI is possible. Additionally, the command `cable privacy bpi-plus-policy total-enforcement` was entered to force all modems to do BPI+. After re-powering the diagnostic modem, it will perform the cable modem registration process again. The CM will be online, but it is not allowed to pass traffic over the cable network. The issue in this particular lab is the transition time. At normal registration the CM is allowed to pass traffic over the cable network (otherwise it cannot get the IP, configuration file, etc.). Only after the expiration of the BPI+ establishment timer (usually 30 to 240 seconds) the CM gets blocked at the CMTS. Thus, a malicious modem still has a little bit of time to do malicious activities, without being authenticated using certificates or exchanging encrypted traffic.

A second scenario was also performed using the deactivation of certain modem features in the configuration file. Therefore, the attack relies on the fact that using an altered CM configurations is possible. The DOCSIS specification allows certain feature of a modem to be disabled using TLV 5. The CMTS is not aware of the CM capabilities until the modem sends its first registration request (which is after getting the configuration file, IP assigned, time, etc.). Therefore, the configuration file can be used to disable certain capabilities of the modem. The modem capability options in the configuration file are also not sent back to the CMTS and thus are also not included in the (keyed) CMTS-MIC calculation. The security features of the CMTS were set to enabled, but not to enforced. The altered configuration is shown in listing 3.11. Now the configuration is regenerated using the tool docsis and the modem is repowered to download the new configuration during the registration process. To check the received capabilities, the CMTS was queried. Listing 3.12 shows the capabilities received by the CMTS for the diagnostic modem. The result was also a BPI+ disabled CM, which could communicate at the cable network (with security disabled).

```
1 Main
2 { NetworkAccess 1;            /* enables packet forwarding */
3   ModemCapabilities
4   {
5     BaselinePrivacySupport 0; /* disable BPI feature at the CM */
6   }
```

```
7   UsServiceFlow              /* creates an upstream service flow */
8   { UsServiceFlowRef 1;      /* SF number */
9     QosParamSetType 7;       /* activates SF */
10  }
11  DsServiceFlow              /* creates an downstream service flow */
12  { DsServiceFlowRef 2;      /* SF number */
13    QosParamSetType 7;       /* activates SF */
14  }
```

Listing 3.11: CM config (CM BPI feature turned off)

```
1  MAC Address                    : 0011.2233.4455
2  IP Address                     : 10.0.1.15
3  ...
4  MAC Version                    : DOC3.0
5  QoS Provisioned Mode           : DOC1.1
6  Enable DOCSIS2.0 Mode          : Y
7  Modem Status                   : {Modem= online, Security=disabled}
8  Capabilities                   : {Frag=Y, Concat=Y, PHS=Y}
9  Security Capabilities          : {Priv=N, EAE=N, Key_len=}
10 ...
```

Listing 3.12: Security capabilities (disabled) received at the CMTS

Countermeasures An easy mitigation is to set the security features to mandatory at the CMTS. Each subscriber in the cable network must enable the strongest security capabilities to be able to use the cable network. The big downside of making it obligatory is the exchange of all old equipment which is not capable of these security features. This is truly a big problem, because of manageable amplifiers and old customer modems (they might have a 24/7 SLA or special requirements at the modem, e.g., L2VPN). To avoid this all or nothing behavior regarding privacy settings, DOCSIS introduced enforcement policies for the CMTS. With the introduction of BPI+, the choices at the CMTS can only be to allow fully compliant and enabled CMs to get online or also to allow older modems access to the network with lower security measures (BPI, which has no secure authentication of modems). The following listing gives an overview of the choices in the case of the Cisco lab CMTS, which are also stated in the DOCSIS 2.1 BPI+ specification [37]:

- BPI+ is required for all capable modems with BPI+ enabled (policy 1), downgrade attacks will work
- BPI+ is required for all DOCSIS 1.1 and later modems with BPI+ enabled (policy 2), downgrade attacks will still work
- BPI+ is required for all DOCSIS 1.1 and later modems (policy 3), above downgrade attacks may not work

- BPI+ is required for all modems and thus BPI only or no BPI -enabled modems are not allowed, the attack will not work (policy 4)

The command `cable privacy bpi-plus-policy` is used to configure the policy. It must be entered on each of the primary cable interfaces of the CMTS.

Moreover, with DOCSIS 3.0 EAE policies got introduced [41]. If EAE is enabled, the CMTS will have to support the enforcement of different policies to allow or deny access to the network for a CM, depending on the capabilities of this particular modem. The improvement using EAE is the establishment and checking of the policy before the CM registers at the CMTS and thus improve the overall authentication and authorization mechanism. A conforming DOCSIS 3.0 CMTS must support the following enforcement policies [41]:

- Disable EAE (policy 1), downgrade attacks might work depending on BPI(+) enforcement
- Enforce EAE on DOCSIS 3.0 modems (policy 2), DOCSIS version detected at PHY level, therefore very secure and downgrade attacks are probably not working anymore when the modems register with DOCSIS 3.0 PHY features (but DOCSIS 2.0 and below CMs will still be an issue)
- Enforce EAE on capable modems (policy 3), downgrade attacks might still work
- Total enforcement for all modems (policy 4), no legacy hardware allowed and therefore downgrade attacks will probably not work

Another problem are insecure cipher suites. A cable modem also sends the supported security ciphers in the registration phase. Therefore, also this choice for ciphers might introduce downgrade attacks. A modem can still try to establish BPI(+)/EAE with the least secure encryption algorithm. Even though DOCSIS 3.0 SEC requires supporting AES as cipher. Regardless of the EAE and BPI+ enforcement, a modem may still provide a supported cipher list containing only "DES 40 bit" to the CMTS. Therefore, in the most cases, a downgrade attack to a more insecure cipher is very likely to succeed. The Cisco CMTS supports a precedence list so that it will take (hopefully) the most secure cipher supported by a particular modem. In any case, the command `cable privacy encrypt-alg-priority aes128-des56-des40` should be used to configure the usage of AES 128bit with most precedences and otherwise the less secure variants of DES. In the case of the Cisco CMTS, there is no way to exclude encryption algorithms and thus downgrade attacks might be still an issue (even with security settings set to mandatory).

The enforcement policies are a very nice tool to enhance the security, but there might be cable modems in the network which have problems and are not fully DOCSIS compliant. Also, old hardware, which cannot be easily swapped out might work with low or none security (BPI/EAE) enabled. This might be one of the biggest issues for real cable

providers. Therefore, total enforcement or even capable enforcement is not possible. This problem can be mitigated by a more intelligent monitoring system. It can track modems which have no security measures or insecure ones enabled. Also insecure chosen cipher suites can be checked by a monitoring system. The system can compare the security applied at the moment (received from the CMTS), with the one stored in a database to determine possible downgrades. This will also help, if there are problems after software upgrades (which might result in broken cipher suites or authentication issues and falling-back to no EAE nor BPI establishment).

3.2.3. Other issues and improvements

This section covers fundamental improvements for a typical cable network. There are still more attacks possible, due to simple network vulnerabilities because of numerous protocols involved into DOCSIS. Some of these issues are covered in the newer DOCSIS standard, which will be stated shortly below. Moreover, improvements to the headend and provider network, such as performance and bandwidth balancing, are covered next.

3.2.3.1. Network enhancements

Customer satisfaction is surely one of the main goals for providers. Therefore, the resources (frequencies, available channels, etc.) must be adequately used to meet certain criteria (e.g., ISM frequency-bands are avoided). In the next segment load balancing to spread the load of the modems, modulation profiles to make a trade-off between reliable and fast bandwidth and simple network issues are stated.

Load balancing Due to the shared network architecture of cable networks and their success in providing internet access, the overbooking might be too high, and customer experiences decreases. To obtain the needed bandwidth needs multiple downstream and upstream channels can be provided on different frequencies on a single coax cable. The distribution of the cable modems and their bandwidth is therefore very relevant to achieve the best distribution of the traffic. When multiple downstream and upstream channels are provided to a node (a bunch of cable modems), load balancing can help to use the available bandwidth efficiently. Not only bandwidth distribution could be the reason to move a modem from an overcrowded downstream channel to another. It might also help to meet SNR and MER goals at the headend. A particular upstream channel (frequency) might be worse than another, and therefore the CMTS may decide to move a CM from one upstream to a different one. The easiest way to achieve static load balancing is to specify the downstream frequency and the upstream channel in the cable modem configuration files. Of course, this is not a very practical way, and

bandwidth load is highly dynamic. The goal is to move the modems dynamically. With DOCSIS 1.0 this was not possible because a downstream channel change forces the CM to reinitialize and thus a non-negligible downtime. Most CMTS support the load balancing with the help of dynamic channel change messages, which were introduced in DOCSIS 1.1 [36]. Of course, modems may still experience a downtime, of a few seconds, because they need to do the ranging process. With DOCSIS 3.0 load balancing is now seamlessly possible [45]. The newer standard certified requires CMs to support at least four downstream and four upstream channels, which can be individually controlled. Of course, depending on the actual modem type (especially the RF tuner), the frequencies must be in a defined range (e.g., first and last downstream channel must be in a 40 MHz window), but newer modems also support full frequency band capturing and thus the channels can be spread around the entire coax RF spectrum. The CMTS may send a message to a CM to change one of the downstream and/or upstream frequencies to another. Because of the parallel working channels of the modem, it can move only a part of the downstream and/or upstream channels and is able to receive and transmit data in this transition time using the available synchronized channels. To do the actual load balancing, CMTS vendors have developed numerous of features to create load balancing rules. A CM can only be balanced within a balancing group, which is in most cases a fiber node or hub (e.g., a street or some streets, which have common downstream and upstream channels connected to one of the DOCSIS line-cards at the CMTS). The main decisions are when to move a modem and which frequencies can be configured.. Cisco offers the ability to decide this based on the CM count, on the utilization, or depending on service flows [47]. In a real environment the load balancing helps a lot to keep up customer satisfaction and to meet SLA goals, but it must be considered, that a particular CM may have problems in using a particular frequency (e.g., bad SNR due to cable issues). Therefore, a failure rate should be configured to avoid an endless loop of changing an erroneous CM to another channel. To prevent attacks the downstream and upstream channel change DOCSIS management message requests have a keyed (derived from authorization message during BPI/SEC registration) message digest, which is used to authenticate the sender. This HMAC calculation is dependent on the Auth key, therefore, also a sequence number is used to select the current Auth key. The change requests (coming from the CMTS), may have a SAID substitution and a service flow substitution in it (encoded as TLVs) due to physical change of the upstream and/or downstream channel.

Payload header suppression In DOCSIS 1.1 PHS got introduced. The feature removes duplicate data in protocol headers and thus increased the usable bandwidth for payload data. The economized data may be source and destination addresses, flags, TTL counters and protocol identifiers. The CM identifies information, which will not change between data transmissions. PHS supports the suppression of headers on layer 2, layer 3 and layer 4 of the ISO/OSI model. The CM sends the replaced header content

(including the length of the field and value) to the CMTS, which is also known as PHS mask. Now the CM will not send the full header, if it detects the content in the headers again, it will send a modified packet to the CMTS, which contains only a reference to the PHS mask. The CMTS will replace the PHS mask in the received packet with the already known content. The data can now be normally handled, e.g., it can be forwarded to its destination. [53]

Modulation The throughput depends highly on the usable channel bandwidth, modulation and error correction. Therefore, this topic is shortly covered in this section. In the downstream direction only two modulations, 64-QAM and 256-QAM with a fixed channel width (NTSC region roughly 6 MHz, or PAL roughly 8 MHz) are specified. Due to the fact that many digital TV channels in Europe use 256-QAM, it should be no problem to also use it for the DOCSIS link, although it requires a better SNR level compared to the 6 MHz wide channels in the US regions. In the upstream path many modulation schemes are defined (until DOCSIS 3.0 QPSK, 16-QAM, 32-QAM, 64-QAM and 128-QAM) which can have channel widths between 200 kHz (baud rate 160k) and 6.4 MHz (baud rate 5.12 M). Due to the ingress problem in the upstream direction providers often use lower orders of QAM modulation or even QPSK (if there are many sockets physically connected to one upstream port). With DOCSIS 3.1 4096-QAM (and optionally 8192-QAM) and OFDM modulation schemes are introduced, which should extend the available throughput, but may require higher SNR (in the case of OFDM it might allow higher bandwidth with lower SNR compared to QAM or QPSK). Another thing to consider is burst noise. Modern switching power supplies and other electronic goods (e.g., electrical motors) may cause errors in the data transmission path. To avoid erroneous data at the destination interleaving is used for electric burst noise. The data is spread around so that the received data containing errors is spread over time. The downside of interleaving is the increased latency, due to the recovery of the spread data. The error correction (until DOCSIS 3.1 mainly FEC) can recover distributed faulty information very well. Unlike interleaving, FEC (DOCSIS 3.0 Reed Solomon) adds overhead to the data. The used modulation, bandwidth and error correction is always a trade-off between robustness, speed and latency. Of course, a provider should configure to support the worst cable link. Constant monitoring signal levels is important too.

Pre-equalization Due to the structure of initial CATV networks and their optimization in the downstream path, the other direction (upstream) has lots of signal issues. Ingress is the most dominant factor regarding low SNR at the CMTS in the provider headend. The main reason is the amplified summed-up noise coming from the connected customer devices (e.g., CMs, but also TV set if they are connected to upstream enabled sockets). Also, the amplifiers itself, cables and (lose) connectors with bad shielding add noise to the signal. To mitigate the increased noise at the CMTS, pre-equalization got introduced in DOCSIS 1.1 and got improved in the later version. The feature also

mitigates other RF impairments such as frequency response, micro-reflections and group delay. The basic working of pre-equalization is an easy approach. The CMTS analyzes the received signal from a particular cable modem. If it can be enhanced, the CMTS sends messages to the cable modem to adjust the current pre-equalizer values. The pre-equalizer basically adds defined amounts of delay to specific components of the signal. The CM applies the new values and uses them to send a pre-distorted signal. This altered signal is transmitted in the cable network back to the CMTS and thus is back altered to its nearly perfect look. When the signal is received by the CMTS, it will look very similar to a near-ideal one. This process is repeated with a delay of 30 seconds to constantly increase the signal clarity and to adapt to network changes. The feature is usually very easy to activate, e.g., on Cisco the command `cable upstream X equalization-coefficient` (X for upstream channel interface) is issued. [95]

3.2.3.2. Network attacks

This section covers general network problems, which might lead to vulnerabilities and denial-of-service attacks. Moreover, management attacks might succeed in the case of default DOCSIS configurations applied (especially to the SNMP agents in the CMs).

Pure CMs A normal cable modem can be seen as a layer two device. Therefore, most of these layer issues are also relevant to cable networks. The behavior of a cable modem is like a bridge, and therefore the broadcast domain is enlarged with this device. Moreover, if two cable modems are connected to their customer interface (e.g., using a cross-over network cable connected to their Ethernet interfaces) a broadcast loop is formed, and a broadcast storm will occur. This simple attack can be seen as a Denial of service attack because it is very likely possible that the used DOCSIS RF channels of the modems will be the same. Of course, this attack will only succeed if both modems are in the same layer two network and thus are on the same line-card or (downstream) channel of the CMTS. However, this very much depends on the actually used CMTS (there are bridge-only CMTS available), and its configuration. However, if this attack is executed on the same cable socket it is very likely that both modems will use the same CMTS and the same line-card and thus this attack is very likely to succeed. A very basic countermeasure is the use of STP. All modern modems and cable modem termination systems support STP (e.g., through SNMP, it is included in the DOCSIS MIB) and the specification also forces the manufacturers to include this feature in their products to be DOCSIS certified or compatible [39]. In any case, it has to be considered, that the CMTS should be configured with a high priority so that it will always be the root bridge.

Modem stack The cable modem is not only a simple bridging device of the two lower layers between the RF cable and the customer equipment (CMCI, usually ethernet). Due

to the cable modem registration process and the management ability of the CMs it has a lot of higher level (e.g., SNMP application layer) functionality built in and thus also a TCP/IP-Stack in it. This increased feature list (besides a bridging modem) makes it more complex and results in a bigger attack vector. The management functionality offers the most dangerous vulnerabilities (e.g., configure the device and subscription parameters or disable it and thus results in a DoS) and thus must be restricted. All advanced functionality of the modem should be available only to the provider (provisioning and management system). Therefore, firewall rules on the CMTS and also on the modem itself help to minimize the potential of successful attacks from the customer (via CMCI) and from the public internet (e.g., via the management IP and functionality of the modem). The customer should have no access to the management of the modem, and therefore all traffic to the whole modem IP network can be blocked (e.g., on the CMTS and on the modem). The same is true for the public internet. Therefore, private IP ranges can and should be used in the provider network for the management of the modems because the other routers in the public internet should not forward traffic to this IP network. Nevertheless, due to proxies or other attacks (e.g., via tunnels), it might be possible to reach the cable modem management network from the public internet. Therefore, also the provider firewall (or internet upstream router) should have rules for blocking these types of traffic. Another reason to restrict the traffic is to limit the features of the modem. Due to the small hardware and thus also small computing power (regarding higher-level application features) cable modems might be very vulnerable to high load attacks (such as DoS). This is very important because in the newest DOCSIS 3.1 technology very high bandwidth speeds and also high packet per second rates are possible. Thus, smaller devices (like IoT and cable modems) can be easily overloaded with SYN or other flooding techniques) and no user data traffic can be exchanged anymore.

MAC domain improvements The (routing) CMTS and the directly connected devices (CMs and CPEs) use ARP (or ND for IPv6) for IP address resolution. Finding the MAC addresses to the corresponding IP works by sending ARP requests as broadcasts, which are sent to all devices in the same broadcast domain (all connected CMs and CPEs at the CMTS interface). The devices receive the requests, process them and may send a response (their MAC address to the given IP). In the IPv6 case, this works analogous, but a multicast approach is used. DOCSIS splits the media into downstream and upstream with a central traffic coordinator, therefore the CMs (and CPEs) cannot directly perform the resolution. The CMTS is involved in ARP. If it receives a request and does not know the IP, it may echo the request and thus sends a broadcast to the connected DOCSIS devices in the downstream direction. A device may send a response back in the upstream direction, and the CMTS may echo this request again so that the requested device knows the MAC address to the given IP. The CMTS may also work as a proxy. Due to the cable modem registration process and other traffic (management traffic, user

traffic, etc.), the CMTS knows many MAC addresses and can answer some ARP requests directly. The CMTS may also bridge requests and responses to other interfaces (e.g., to a bridge CMTS, other DOCSIS interface, etc.). The modems connected to one logical CMTS interface form a relatively big broadcast domain (usually in the range from 50 to 500 CMs). Therefore, the ARP traffic can be quite huge, due to the connected devices which may have viruses or act badly (e.g., IP scanner, devices not following RFCs) and thus the CMTS load increases. The CMTS resources can get overloaded due to ARP, which results in a disrupted service because nearly no legitimate data traffic can be handled on the DOCSIS network anymore. The amount of ARP packets can be limited at a DOCSIS 3.0 (or higher) CMTS to minimize the impact of high ARP traffic (e.g. on Cisco the feature `cable arp filter request-send packets/time-unit time[seconds]` and `cable arp filter reply-accept packets/time-unit time[seconds]` can be used to set the ARP limitation). [41]

On a Cisco CMTS the command `cable arp filter` can be used to control ARP traffic. The feature is configured at the physical DOCSIS channels (not on a bundle and thus allows a fine grade adjustment of the limits per physical domain sizes). It specifies how many ARP packets are allowed to pass in a given time per SID (and thus on a per-modem basis). [12]

Management attacks

The DOCSIS MIB of the CMs offers a feature-rich functionality. Bandwidth speeds, firewall rules, DOCSIS channels and many more settings can be manipulated at a CM using SNMP. Therefore, it is very critical that only the monitoring system (or whatever provider system) has access to the SNMP agent. Firewall rules at the CMTS as well as at the CM can avoid security issues. In a normal environment, a CPE (or the CM itself) doesn't need to have access to the other hosts in the management IP network (except to the management station and provisioning system) anyhow. Therefore, blocking this traffic is, in general, a good idea in order to minimize management attacks to other CMs in the network. It is also very important that only the DOCSIS MIB is reachable via the DOCSIS RF interface of the CM. A provider might be able to snoop local customer traffic (e.g. traffic seen at the customer side of the CM) or get other sensitive data (e.g., which data type is being transmitted or received). Therefore, the CM firmware implementation must assure that the access through the DOCSIS RF interface to the SNMP agent is limited to the DOCSIS MIB. [35]

The CMTS also offers a big SNMP MIB analogous to the SNMP agent in the CMs. Therefore, this access should also be controlled (apart from good access credentials used in SNMP). In general, the CMTS SNMP agent needs only IP connectivity to the monitoring and management provider network and not to the CM management network.

A firewall rule on the CMTS, which blocks all access from the CMs management network to the CMTS SNMP agent can, therefore, be placed to increase SNMP security.

Chapter 4.

Additional security concerns in DOCSIS networks

This section covers security issues of cable networks, related specifications, and implementation issues. The presented vulnerabilities are not exploited in the lab. The issues are grouped into physical attacks (e.g., changing the network infrastructure and consequences regarding data transmission security), passive attacks (e.g., decrypting traffic) and active attacks (e.g., data manipulation, man-in-the-middle attack, etc.). Moreover, the impact of implementation issues and legal considerations are evaluated.

4.1. Physical attacks

The traditional cable TV networks had a seal at the handover point, where the CATV cable entered the homes. This was done to restrict the redistribution of the signals to non-paying subscribers, which was the main threat. When the networks also allowed upstream data communication things changed a lot, but the original threat model was not correctly adopted to this massive change of the information flow. Customers can usually plug and unplug their modems by themselves, which can already lead to problems. Moreover, manageable amplifiers are going to be a security risk due to the built-in software capabilities. New DOCSIS features increased the signal quality, but also side effects and issues evolved, which are further discussed in this subsection.

4.1.1. Cable modem swap

Cable modems are usually treated as customer premises equipment. Self-installation is one of the most common ways to install internet subscription nowadays and therefore most CATV providers allow the customers to connect the devices themselves. The subscriber is in general allowed to disconnect, reconnect or attach the device to a CATV socket and to a power outlet. Therefore, it a CM swap is treated like a normal TV replacement. This also applies to the threat model of the CPEs. There may be

providers which seal the coax cable to the modem using a physical protector (or the whole device including the connectors) so that the customer cannot easily alter the hardware installation, but this is not the usual case for large providers in Europe and the USA. [30]

Cable modems need access to the cable network, also in the upstream direction. The CATV socket must support this. Each interface to the upstream path increases the received noise at the headend. If the noise is too high, no information (the upload data from the CMs) can be received and handled at the CMTS. Therefore, bad noise coming from a customer CATV socket can lead to a denial-of-service attack, because it can also affect other customers. The reasons can be a defective modem, a loose connector (which injects the surrounding signals into the CATV network), or a malicious person injecting wrong signals on purpose. [30]

A malicious person may also swap the modem with another one. The new modem might allow different services or might not behave according to the DOCSIS standard. A diagnostic modem may be used to attack the network in many ways (e.g., denial-of-service, cloning, etc.). Therefore, most providers do not allow all modem-models on their network. Typically, a list of accepted modems is published. Another reason for doing so is to minimize the training of the help desk staff because they only need to know the common problems of the listed devices.

Another attack is to manipulate the physical infrastructure before the modem. Some providers use filters to allow only distinct frequencies to the customer. This might be due to the chosen subscription (e.g., TV channels 1-20, best effort internet) or due to the legal considerations at a given place (e.g., some frequencies are forbidden by the government). These providers use frequency-filters to hinder use of the blocked frequencies. A malicious person may remove such devices (which are typically in the path between handover point and CPE, e.g., between CATV outlet and cable modem) to increase their service level (e.g., higher speed due to less crowded upstream, enable hidden channels). [31]

4.1.2. Manageable HFC devices

The HFC signal distribution network consists of many devices, one type of those are line amplifiers. They are used to mitigate the signal loss of the distribution cables, connectors, and taps (usually junctions to regional amplifiers for a smaller number of subscribers) and connect the headend to the streets distribution. Analogous to the outdoor coax amplifiers are node amplifiers, which have on the one hand a fiberglass connector (coming from the headend) and on the other the coax output for a particular node. This node amplifier is usually used for several hundred homes. Of course, these amplifiers are also bi-directional to support data communication using DOCSIS. Both amplifier types are essential for the whole HFC network. Because of the coax cable characteristics the

attenuation and frequency behavior of the cable change with temperature and other environment properties. In order to accomplish this task, automatic gain correction can be used. The output signal derivation of the distribution and node amplifiers need to be in a very tiny range because attached home and transition point amplifiers are adjusted to these signal levels. If there is a change in the output signal level of the distribution amplifiers, it will also change the output signal of home or amplifiers nearby the customers, which will finally result in a considerably changed signal at the CATV outlet. Moreover, many distribution amplifiers offer manageable features, like setting the desired signal output level, signal error statistics (egress and ingress control), set output port state and many more [27]. To perform this management, the devices include a DOCSIS modem to have access to those features from remote (e.g., headend) [25]. This device can be provisioned like a normal CPE cable modem and behave similarly. The management features are mostly offered through an enhanced SNMP agent (beyond the normal DOCSIS MIB) or offer a webservice.

There exist other products which also offer a built-in DOCSIS modem. Outdoor cable modem line monitors are used to verify the signal quality at some important points in the CATV network [33].

Unfortunately, most (if not all, at the time of writing) of such manageable distribution devices contain only a DOCSIS 1.1 or DOCSIS 2.0 modem. Therefore, they are vulnerable to some attacks. The following list provides some scenarios, which will eventually lead to serious security or network issues:

- Sniffing the information: Disclosure of the data from the headend to the device with the built-in CM (and maybe also the reverse direction), if the traffic is not or not well enough encrypted. Due to the use of DOCSIS 2.0 or lower, BPI+ is the best option for data privacy, which only offers the outdated DES cipher.
- Cloning the manageable device: The MAC address and other relevant information (e.g., DOCSIS version, supported feature list, etc.) is broadcasted in an unencrypted way on the specific DOCSIS node and thus readable at all CATV outlets.
- Management attacks: Due to the built-in DOCSIS modem functionality the device offers an SNMP agent. The access to it is not restricted at its default, and thus a malicious person can alter and read settings from the device.

To mitigate most of the issues, it is important not to handle manageable distribution devices like normal customer premises equipment. The remote communication must be done using side-channels. Of course, it would be the best option to use a physically separate connection to make the information exchange as secure as possible, but this is not practical. Another option is to use different downstream and upstream channels. The downside is the resources being used, an extra DOCSIS DS and US port at the CMTS will be occupied for the manageable devices. Nevertheless, the signals are still

being amplified and received at the CATV outlets at the connected homes. Therefore, frequency filters must be used to hinder the frequencies reaching the customers (e.g., at the output port of an amplifier). Moreover, the headend and (modular) CMTS firewall and provisioning must also handle the devices properly. They usually don't need an internet connection and the access to the SNMP agent must only be granted to the monitoring and management system of the provider.

4.1.3. Pre-equalization

Since turning the cable plant into a bi-directional communication media, ingress has been one of the biggest issues. One reason is the amplification of unwanted signals to the headend. They come from the CATV outlets, impairments, bad cables and connections. With DOCSIS 1.1 the pre-equalization feature was introduced to compensate for such problems. It adjusts the upstream signal of cable modems according to the received signal at the CMTS upstream port. The consequence is a better signal received at the CMTS, thus improving overall performance (lower bit error rate, and thus higher CM capacity per upstream port). The CMTS looks at the signals coming from the modem, and sends adjustments (new pre-equalization coefficients) to the modem in ranging messages. The CM applies the new values to its equalizer taps, which are delaying and components in the signal generation process. The CMTS may send equalizer-data again to the CM repeatedly (until it decides that the signal cannot be improved with pre-equalization). Apart from the upstream signal alteration, the feature also makes it possible to use cable modems as monitoring tools. The values of the equalizer inside each CM can be displayed using SNMP and is thus also readable at the headend and can be easily monitored. This gives a big advantage, compared to the limited signal indicators at the CMTS, which can only display the upstream quality of a CM, because the CMs can also report there downstream signal quality. [100]

The equalization information can be used by various parties. Some usage scenarios are further stated in the list below:

- Provider: When pre-equalization is introduced, the SNR (signal noise ratio) on the upstream increases significantly [100]. Therefore, more cable modems could use one CMTS upstream port and thus a higher number of cable modems can be supported by a single CMTS. Another benefit is the monitoring capability. The DOCSIS MIB was enhanced to support various signal indicators to be remotely displayed (e.g., micro-reflections, group-delay, etc.). Using pre-equalization additional information can be determined, such as the type of impairment, like corroded cables and other issues, and the estimated distance to the impairment. This makes troubleshooting much easier. Technicians can be sent to the estimated location of the problem and don't need to start at the homes, where the cable modems do not work. Moreover, work was done by Charter Communications and CableLabs to efficiently collect

pre-equalization data from nodes and how it correlates. The outcome was a normalization of the data and information about which field problems fit those values. The next step is to detect problems before customers are really affected. The monitoring values of the cable modems and amplifiers (e.g., nodes, distribution amplifiers, etc.) may get worse. Of course, intelligent monitoring systems, which actively relate monitoring values to saved known normals, can detect problems very quickly. The overall outcome of these investigations was pro-active-network-monitoring. [43]

- Customer: The major goal of pre-equalization are less upstream issues. Even if old cables are used, which have a very bad signal connection, upstream communication is mostly still possible, which would usually not work without pre-distorting the signal.
- Attacker: Although pre-equalization offers really great benefits, it can help malicious persons. It may be possible to make a rough estimation of the distance from the CMTS to one particular cable modem. A reference point might be used to calculate the rough position of a particular cable modem based on this reference. A malicious person may now watch if there is traffic from or to a particular cable modem. If there is no traffic, the malicious person knows the location and may harm the home (e.g., by stealing where the cable modem is located).

4.2. Passive attacks

This section covers theoretical attacks and issues of encryption data mechanisms in DOCSIS. The issues described in this section may lead to easier decryption attacks or even make the performed cryptography completely useless. Moreover, capturing data coming from the modems (upstream sniffing) and its consequences are mentioned. The most relevant factors, which makes upstream sniffing harder, are stated, and the probability in certain scenarios is evaluated.

4.2.1. Deciphering the downstream traffic

Most of the DOCSIS networks still use DES as packet data encryption algorithm. Therefore, the first part focuses on deciphering 56 bit DES keys (TEK) PDU decryption without having the private RSA certificate nor the authorization or key encryption key (which are used to protect the PDU key). The mode in which the DES algorithm is used is cipher-block-chaining (CBC). Therefore, an initialization vector (IV) must be used for the first block to encrypt. DOCSIS requires to re-initialize each frame with the actual used TEK and corresponding IV. This means identical plain-texts will have identical cipher-texts (IV will be re-used). The success of an attack also depends on the lifetime of the keying material. Because the TEK (with its parameters, like IV)

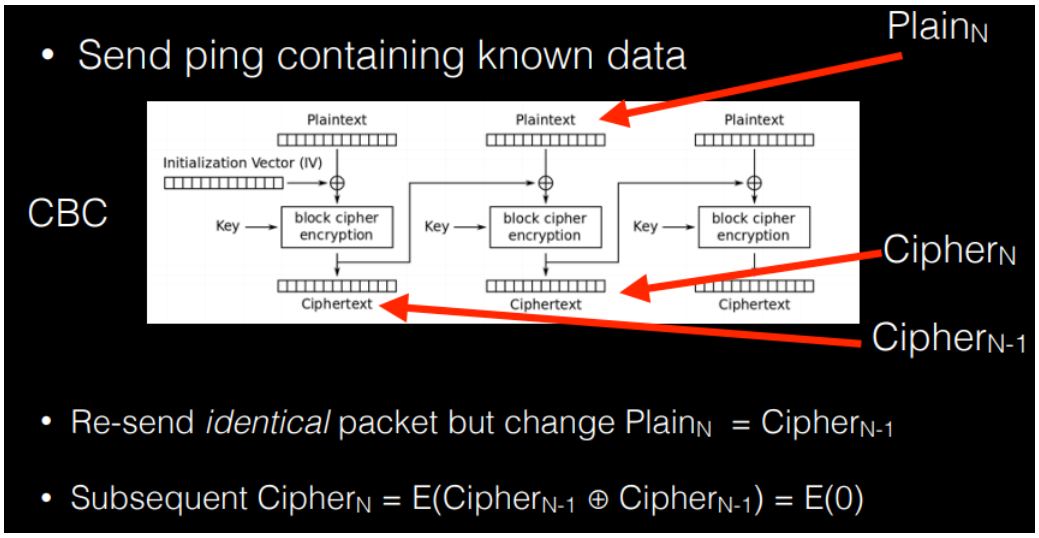


Figure 4.1.: Obtaining known plaintext values [97]

has a limited lifetime of some hours (default 12 hours), it makes it very vulnerable to the below-mentioned attacks. The specification states exactly the lifetimes of various parameters of the BPI/SEC specification part. Moreover, the attack is also possible without being a subscriber. A CATV outlet to passively sniff the traffic is sufficient. This keeps the chance of malicious persons being detected at a minimum. [96]

DES brute force The first attack is a brute force attack using rainbow tables to benefit from a time-memory trade-off. Although this attack sends data to the victim it is considered as passive, as no data must be sent to the victim from the inside of the DOCSIS network, nor must the attacker be a subscriber. Basically, the first step is to determine the victims and produce MAC-IP tuples of the CMs. As ARP traffic is not encrypted, it is very easy to do this task, it is practically only a matter of time. Management traffic will occur, and due to some aging and other real traffic, ARPs packets will be sent. This information is also exposed in the first place when the cable modem gets provisioned and if EAE is not used. It is also possible to identify the victims and thus produce the MAC-IP tuples of CMs with an active approach by sending data (e.g., ICMP ping) with known length to CM IPs and making a correlation to the encrypted packet data (also the time can be an indicator). When actively sending data it is possible to perform a known plain-text attack. The first step is to send known data to the victim while sniffing the encrypted traffic. The next step is to send an identical packet, but with block N containing the data of the sniffed cipher block at position N-1. This reveals subsequent cipher N, which is equivalent to the encrypted form of cipher N-1 XORed with cipher block at N-1, which is the equivalent of encryption of zeros. This process is depicted in figure 4.1. [97]

Now there are many possibilities to brute-force:

- EFF DES Cracker [22]
- Karsten Nohl for cracking remotely OTA DES keys using rainbow tables [78]
- Using FPGAs (e.g., Hacking 4G USB modems and SIM Card via SMS [79], which also cracks DES using FPGAs)
- Many more in [17]

Of course, the attack should be very fast, as in the average case the same key is only used for about 12 hours. Due to this, the author in [97] uses rainbow tables, which are created in the cloud using Amazon EC2 on GPU spot instances. Using this lookup tables, it is basically possible to find most of the keys in about 23 minutes. Moreover, the author also uses bit-slicing. Instead of using addition, typical fast operations, like XOR, are used to do efficiently parallel DES operations. Now the encrypted payload (after the MAC source and destination addresses) of the PDU can be decrypted. To decrypt all sniffed traffic the IV for CBC has to be sniffed in the BPKM key reply message, which is sent when the CM requests for keying material by an attacker (at the provisioning step or after the half-time before expiring).

DES CBC insecurity attack Due to the use of CBC mode the security may be negligible because of the high data rates used in DOCSIS networks. In CBC mode DES security will degrade after $2^{64/2}$ blocks encrypted with the same key (where 64 is the block size, which is used for DES with 56 bit key size). Due to the high-speed data communication in DOCSIS, this block count will be easily reached before the end of the actual key (because the TEK lifetime is in the range of some hours). [55]

If a downstream speed of 50 Mbit/s (approx. payload speed for one downstream EuroDOCSIS 256 QAM channel) is assumed the block count is reached after roughly 92 minutes and thus before the end of the usual TEK lifetime. The calculation is as follows: $2^{64/2}$ block-count * 64 bit block-size / 50000000 bit/s = 5497.56 seconds, which equals roughly 92 minutes.

Of course, in a real environment, a customer can get much higher or lower speeds, depending on the DOCSIS configuration file or other bandwidth limitations. Moreover the attacker needs a little bit of luck that the victim consumes many bandwidth resources to obtain the needed data packet count. To increase the probability of the attack success the attacker might change the raid from a passive to an active one by sending data (e.g. ICMP packets, ARP, etc.) to the consignee (the legitimate modem) and thus generates many data packets.

Mode of operation When data frames need to be encrypted, cipher block chaining mode for the chosen cipher is used in DOCSIS. This is only true for data frames which are equal or larger than the block size of the cipher mode. Data frames with less the length of the block size need to be encrypted differently, which is named residual block termination and does not add overhead to the resulting ciphertext because no padding is used. The last small block is generated by encrypting the initialization vector XORing the resulting left-most n bits with the plaintext. It is already stated in the specification that this method is vulnerable to attacks. A simple attack is done by XORing two ciphertexts (encrypted with the same keying material), as it equals to result of XORing the corresponding plaintexts. In most cases, this is not an issue, because for payload customer data the IP header already has at least 20 bytes length. Fragmentation frames are a bigger problem, as they might be very short and a few octets may be recovered using this simple attack. [41]

4.2.2. Upstream sniffing

Although DOCSIS uses only one cable for data transmission, it is a duplex medium. This is accomplished by the usage of splitting the available frequency band into downstream and upstream part. Therefore, in general the same procedure, as for downstream sniffing, can also be used for upstream sniffing. The major difference is the usage of tuners which support the upstream frequency bands and a demodulator for QPSK, or quadrature amplitude modulation. With DOCSIS 3.1, also the use of OFDM is possible and therefore the sniffing hardware must support it. Which type of modulation parameters is actually used is broadcasted in the downstream path periodically using the upstream channel descriptors (UCD). Depending on the chosen hardware various software for capturing and analyzing may be used. The next paragraphs give a quick overview over possible methods for upstream sniffing and their probability in connection to the CATV structure and the components used.

SDR A software defined radio solution is based on a hardware part, which receives the signals and demodulates them and software which interprets the received information. Usually, the overall demodulation can also occur in the software, if the ADC values from the hardware receiver are sent to the analysis software, which may add filters to this received signal. The biggest issue with this solution is the bandwidth and the demodulation. The usual channel bandwidth at DOCSIS 3.0 is typical 3.2 or 6.4 MHz. This is no problem for an HackRF [23] or other advanced SDRs [13]. The biggest advantage is the price of some SDRs. Cheap devices, like the RTL2832, have a relatively small usable bandwidth (typically only up to 2.8 Mhz bandwidth) and a limited usable frequency range (typically starting from 24 to 1850 MHz[84] for the R820T tuner and the DOCSIS upstream can be down to 5 MHz). Therefore, they can only be used if the upstream channels bandwidth is only 1.6 MHz or less and are located above 24 MHz.

DVB receiver In theory, also a DVB receiver may be used to receive the upstream signals. A probably more realistic approach is to use DVB-C receivers with PCI, PCIe or USB interfaces. They can be used by a PC, which decodes the received signals. Of course, the usable frequency bandwidth and other demodulation parameters depend on the actually used receiver model (and the HW revision). The biggest benefit with this solution is the low price, but the usage very much depends on the used hardware (tuner or others). The biggest issue is DOCSIS' own PMD (physical media dependent) sublayer, which defines modulation schemes. The intergap and other modulation parameters are different from those used in DVB.

Cable modems In [97] also the possibility of hacked cable modems is described. Although it is not clear if the whole upstream can be sniffed with some cable modems from the manufacturer Ubee, it can mirror its own upstream data to the LAN interface. This might be interesting for decryption attacks. Newer cable modems (especially those for DOCSIS3.1) may support the use of sniffing the upstream frequencies because the downstream and upstream tuners (and modulators) support a very wide overlapping frequency bandwidth. With the introduction of DOCSIS 3.1 also the frequency usage got enhanced. Upstream and downstream frequency are not necessarily strictly separated into lower and upper frequencies for their usage, higher downstream frequencies may also be used for the upstream path. This means a downstream channel may be tuned to an upstream frequency and it may also be possible to demodulate these signals and therefore making it possible to sniff the upstream information.

Analyzers For diagnostic purposes and problem search there are DOCSIS analyzers [51] [50]. The range of available products varies from simple frequency spectrum view of the down- and upstream frequencies up to upstream and downstream signal generators. Some units also offer the ability to look deeper into the upstream signals to analyze, not only SNR or MER is shown, rather the FEC is evaluated, and the packet error rate is stated. These analyzers often also offer the capability of mirroring this data to a tap LAN port of the analyzer. Of course, this solution is very costly and not easy to get as some of the vendors require being an official cable TV operator to get a unit.

Special hardware There is nearly always the option to use specially crafted hardware for signal analyzing purposes. An self built design with a (possibly also self designed) tuner, modulator, and a DSP or ADC may be connected together to form your own upstream sniffer. Parts to evaluate the signal, like a DSP in conjunction with a FPGA can be used to sniff the signals and get a meaningful output data. Of course, this device would basically be equal to your own SDR, so the complexity is quite high, and the cost of development, production in conjunction with software creation is very high.

Sniffing probability If the upstream direction has the same properties as the downstream, the probability of sniffing upstream signals would be exactly the same as in the downstream case. This is also true if we consider the grid of cable modems connected with the CMTS as a broadcast line, but this is only true for the logical connection. The main issue with only physical connecting three points (simple two-way splitter) is the decreased SNR and the ingress (noise or other signals from one of the connected devices or even the open socket itself). Each connected device adds massive noise to the system. In the case of a broken device, which may emit noise, it can harm all other components. Therefore, a real CATV based DOCSIS network is based on splitters, taps and other connector circuits with direction effects. These directional couplers are used to steer the upstream and downstreams depending on the usage of the port in the right direction. The effect is a less decreased SNR, better immunity for noisy devices and also a higher received upstream signal level at the CMTS. Of course, this behaviour makes the sniffing part for upstream signals harder, which may help to avoid misuse by maliciou spersons.

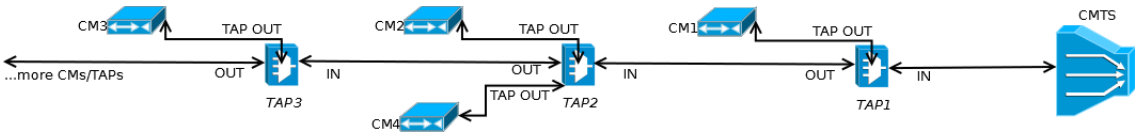


Figure 4.2.: Simplified cable plant example

The mentioned issues and how they influence the sniffing probability are now being analyzed at an example. Figure 4.2 shows a very simplified cable plant, with one CMTS downstream/upstream port connected to four cable modems (which are connected via taps, like in a real cable plant). The taps help to decrease ingress and keep up immunity (high SNR, low bit error rate) of the cable plant. It keeps the noise coming from the homes, amplifiers, TVs, cable modems and other sources at a minimum. Let's assume a malicious person wants to sniff the upstream signals at the socket of cable modem two (CM2). It is obvious that it can only do this at the same physically connected segment, which is mostly equal to a fiber node output. To come to a real estimation of the signal values and the probability of sniffing the cable modem upstream values are considered to be +45dBmV (due to minimal recommended values of a SB6183 cable modem [4]). The taps are all two-way junction boxes with 20dB attenuation at a tap socket and 25dB isolation (tap to tap, product: PCT-G2-20 [26]). Port isolation refers to the effect of attenuating the signal of a splitter or a tap between two outputs. Return loss is an attenuation of the received back signal on the input of a splitter or a tap. Cable modem two will probably receive upstream signals from the following sources (only the main attenuators are mentioned and counted):

- CM4: Attenuated by approx. 25dB due to port isolation (perfectly receivable)
- CM3: Attenuated by approx. 65dB due to tap3 drop (20dB), port isolation on tap2 (25dB) and tap2 drop (20dB)
- CM1: Attenuated by approx. 80dB due to tap1 drop (20dB), a mixture of port isolation, return loss (40dB) and tap2 drop (20dB)

If the same characteristics are assumed for the upstream signal sniffing tuner as for the downstream tuner, the probability is as follows:

- -15dBmV and higher is the range for a perfectly received signal
- -20 to -15dBmV is very likely legible (mainly depending on signal SNR)
- -40 to -20dBmV possible with a good amplifier, but still difficult or impossible (very depending on signal SNR)

The result will be a perfectly received signal for CM4's upstream data (+45dBmV sent from CM4 - 25dB drop gives +20dBmV). In the case of CM3 it is a bit worse and counts up to -20dBmV (+45dBmV sent from CM3 - 65dB drop gives -20dBmV). This will very probably still be legible. CM1 is in the best case of not being sniffed because it has the most attenuated power (being seen from CM2). Due to the high return loss (varies from tap vendors) the signal is received at approx. -35dBmV, which is in the most cases too low to be readable directly. If special hardware is used, e.g., a very good signal analyzer, it may be still receivable. Another solution is to also increase the signal with an RF amplifier, but this requires a high SNR received at the signal input of the amplifier and low noise at the amplification (uncertainty of the hardware parts will probably drop the signal SNR). The above-mentioned probabilities are mainly counted due to the received power signals. Also, the SNR and other parameters (like the MER) will count and influence the probability, but not as much as in the downstream, due to the usage of lower modulation orders. Small variations in the real environment will exist due to the imperfection of cables, sockets, taps, splitters and other physical hardware. All received upstream signals will be increased due to some more return behavior in the components and may also be attenuated. Moreover, insertion and through loss (approx. 0.8dB) is not considered. Nevertheless, this example shows the high probability of sniffing neighboring CMs upstream signals, if only passive devices (splitters, taps) are in the signal path.

Decoding upstream signals To further analyze the received information the signals must be decoded after demodulation. DOCSIS uses its own proprietary demodulation and media access technique for this task, because many upstream parameters can be configured according to the cable plant and provider needs. For example, different upstream media access algorithms can be used at the CMs. In the simplest situation only TDMA (time division multiple access) is used and MAP messages define the sending

time and amount for each CM, which wants to access the upstream path. The decoding software must consider those messages to extract and match the information to distinct senders (CMs, or SIDs). Therefore, it is evident that it is also necessarily to capture the downstream signals and use the received UCD and MAP messages for upstream decoding. There also exist other types of upstream access. One example is FDMA (frequency division multiple access), which is applied to use the available bandwidth simultaneously for many CMs. The cable modems are typically spread across different upstream frequencies, this also has the benefit of increased SNR at the CMTS (because of the ingress distribution over multiple channels). Also simultaneous access of the upstream path is possible using a scramble approach. The SCDMA access method in DOCSIS uses codedivision-multiplexing and TDMA. It allows multiple modems to use the upstream simultaneously in the same time slot. This is accomplished by the use of 128 orthogonal codes, in which up to 128 symbols can be transmitted. The spreading is done in the time domain. Of course, this information can be recovered by a sniffer, but the initial SCDMA codes and other parameters (slot-number for a CM) are told during registration and in some management messages (e.g. MAP for slot time) and must be used to enable the decoding of the upstream signals for CMs using SCDMA approach. Which upstream channel is mapped to a particular downstream can be found in the downstream UCD message. Moreover, only the primary downstream channels carry those types of DOCSIS management messages. Therefore, non-primary channels can be neglected.

All the solutions mentioned above have issues with multiple upstreams. Since the introduction of DOCSIS 3.0 it has been possible to bind multiple streams into a single logical one. The result is the spreading of data into numerous physical channels. If this technique is used, multiple sniffers (tuners) must be used, and the software must reassemble the data to get the full upstream data information back. Otherwise, the received information may be truncated, damaged or some data packets maybe lost.

4.3. Active attacks

This part describes attacks, which need to send data to a victim or involve hackers actively engaged in the attack execution. Starting with service disruption, more advanced attacks, such as man-in-the-middle, up to network and impersonating security considerations are evaluated. Insider attacks are included too. They understand the cable plant better and thus also know their security aspects (in particular the provisioning process and the monitoring).

4.3.1. Denial-of-service attacks

One of the worst customer experiences is service disruption. The vulnerabilities begin with basic service overload to signal ingress issues. Due to the upstream assignment by the CMTS scheduler and the DOCSIS protocol itself the throughput of the whole system might be gradually less. Many of the higher level layer attacks will work in a DOCSIS network, as they are not specific to the underlying transportation protocol (like simply overloading the receiver or nodes in between with data). There exist also very specific attacks to DOCSIS networks, which are discussed now.

Service overload The DOCSIS bandwidth and the headend have limited resources. Therefore, an attacker may consume an extraordinary amount of resources, so that the usual customers cannot be provided or the available data speed is too little for the subscriptions. Of course, a provider usually overbooks the system to some degree, because usually not all resources are used at the same time [69]. There are many entities in a DOCSIS system, which can be used to disrupt the data cable service:

- Static bandwidth: The modem gets one or more Service IDs assigned during the registration when the device is powered on. If there is no restriction, the CM can use the maximum channel bandwidth. A malicious CM can allocate and produce lots of traffic and thus use all available bandwidth to hinder other devices from communicating. To mitigate such problems each CM (and each SID) should be limited. This can be done by using the DOCSIS configuration file, which states data flows and associated parameters, like the max. consumable bandwidth (also short bursts can be configured) and the priority of the flow. Some manufacturers (e.g., Cisco) offer a feature to limit also static (sometimes also dynamic) SIDs if there is no restriction done in the configuration file.
- Dynamic bandwidth: parallel to static SIDs it is possible to register SIDs dynamically. This can be used for special requirements. Voice over IP services are very common and require low jitter and latency. Therefore, it is useful to give VoIP traffic a high priority and another bandwidth scheduler in a DOCSIS environment. A malicious person may intentionally request a dynamic SID (with high priority) and consume all bandwidth by exchanging lots of traffic. This behavior can be mitigated by specifying the behavior of dynamic SID creation at the CMTS (e.g., only CMs with special DOCSIS configuration file settings are allowed to register specific dynamic SIDs) or a SIP registration must pass the CMTS.
- DHCP server IP allocation: An attacker could fake lots of MAC addresses (CPE or RF-CM) to allocate all free IP-addresses of the cable provider node network. The result is that newly powered-on CMs cannot be assigned with a free IP and therefore will not be able to get online. Of course, the use of unknown CM MAC addresses is only possible if the provider allows the usage of his own cable modems

and offers a self-service installation. The cable provider could specify the CM MACs statically, thus mitigating over-allocating the DHCP by faking a lot of CM MAC addresses. Another solution is to use an IP range of its own for each new device on the network so that it is handled completely independently, thus not influencing other subscribers. A malicious person may fake CPE MAC addresses to hinder other customer CPE devices from getting free IPs. This attack is usually possible with a higher probability because a cable provider does not want to manage all CPE MAC addresses (e.g., PC, router MAC) statically due to the high management effort. Therefore, DOCSIS provides a feature to limit the amount of CPE MAC addresses. At least the DOCSIS configuration file entry MAX CPE entry should be set (usually to 1). Moreover, many CMTS vendors offer additional features to limit the CPE address amount usage. This functionality should also be used to hinder malicious customers (which may use other configuration files) from executing this attack.

- TFTP server: During the provisioning process of a cable modem the DOCSIS configuration file is downloaded from a TFTP file server. If this file could not be downloaded the CM will try to synchronize again and repeats the overall cable modem registration process. An attacker could try to overload the TFTP server to keep new legitimate CMs from getting online. One attack scenario is to download the same configuration file many times and in parallel so that the resources of the application are all being used and new file requests cannot be answered. Another attack might be to try to send other commands (e.g., put or request random file-names, get specific blocks of a file, etc.) very fast, thus overloading the service. Of course, these issues must be considered, because also in the normal operation of a cable network a situation of massively downloading configuration files can occur when one (or more) nodes are re-connected. A firewall and a hardened TFTP server should be used to mitigate such attacks (e.g., the TFTP server may only permit newly synchronized CMs, which are detected by the CMTS, for the max. retry count of 5).

- TIME service: Analog to the TFTP server issue, the same problem is true for the TIME service. The mass use of this resource must be limited by the usage of a firewall and a hardened ToD daemon.

- Monitoring system: A provider should monitor the cable modems to detect problems and may also use the management system to offer services like setting the WiFi password of a residential gateway. A device may also send errors, warnings and other messages to this monitoring station. A malicious person may send many notifications (or traps) to the monitoring station to overload it. To mitigate such issues, the number of messages or the throughput from each subscriber to the monitoring system should be limited.

For each of the service overload issues, a firewall and IDS/IPS system may additionally help to identify malicious activities.

Disrupting TCP flow Most of the regular cable customer traffic is TCP based. In a full-duplex network, with both directions having the same speed and delay time, the flow of data and acknowledgements (which are needed for TCP) is evenly spaced. There is also a settle-point, near the max. available bandwidth, for the data transmission speed. Due to the fact that DOCSIS is a multiple node asymmetric (less bandwidth for upstream) network, data transmission can be negatively influenced (e.g. different delays, bandwidth). One issue is delays, because the CM may get no sending time slot, which causes a disrupted acknowledgement packet flow. The first DOCSIS version had big problems with this, as CMs got a transmission opportunity based on a contention algorithm. SinceDOCSIS 1.1 piggybacking is now supported and therefore also multiple acknowledgements maybe sent in a burst (the CM requests further data transmission opportunities). On the other hand, also splitting larger packets is supported. It is not possible to piggyback future requests in a concatenated frame because the concatenation header excludes the extended header (request additional transmission) of DOCSIS messages. In a real scenario the combination of the DOCSIS concatenation, splitting feature and scheduling (at the CMTS for CM opportunities) debilitates the TCP flow. A Denial of Service attack can be done by pinging or sending TCP SYN packets to a group of cable modem IP addresses, which are connected to the same CMTS. This may cause fewer throughput. The authors in [73]showed by simulation that the collision rate is between 48% to 68% and the downstream throughput dropped significantly from 45% to 10%. The attack can also target one CM, but it will not influence the overall system fundamentally. Another interesting observation is the timing settings of the CMTS. Because of the delayed packets, depending on the size and rate, the map time (when the CMTS tells the CMs there sending opportunities) and the contention time can be observed. [73]

Re-injecting information In theory it is possible to inject data into the upstream path. Of course, there is no physical protection from this. Taps and splitters are electrical components on the lowest layer, like a normal ethernet hub and will not be dropped or filtered, like a layer two or layer three switch will or can do. A malicious person can inject TCP RST packets or ICMP error packets at the right time(e.g., the specific CM got a transmission opportunity) and the connection may die. An attacker can do this by sniffing data and re-injecting it. Of course, if the data is not encrypted, it is also possible to generate data packets of your own with the desired payload (e.g., kill a TCP connection and thus causing a disrupted service). It is also possible to re-inject sniffed encrypted data at the currently active key parameters of the victim. Thisis possible due to the use of the same IV and key in a specific period and due to the issueof replay attacks. [62]

Forge management messages Some DOCSIS management messages are not authenticated, encrypted or irrevocably assigned at the first sending. These types of message can be constructed by a malicious person to disrupt the current operational mode of cable modems. An attacker can send wrong working parameters to a bunch of cable modems, e.g., to change their downstream and/or upstream frequencies to something else. This can be done using a self-constructed DCC (dynamic channel change) DOCSIS management message. The modems will try to register on this frequency, which causes them to have a significantly long (e.g., some minutes) downtime, no normal data transmission will be possible. Another interesting MAC management message is Upstream Disable (UP-DIS). This feature was designed to switch-off the RF transmitter of a cable modem, regardless of the state of its CPE (e.g., if there is a virus on the PC, and it is badly impairing the network) [38]. It may also be used by an attacker to kick-out cable modems. Of course, an attacker needs to send those messages either by impersonating a CMTS message or by having SNMP access (some DOCSIS messages can also be sent by SNMP) to the victims. Therefore, a proper SNMP filter is necessary to keep this attack from being successful and the CMTS to CMs data path must be physically safe (hard to achieve). [55]

Signal injection The upstream frequency path from the CMs to the CMTS is physically always connected. Therefore, ingress noise is a problem in the DOCSIS system. A simple service disruption can be done by injecting noise into the system. If this is done all the time, the CMTS cannot decode (or demodulate) any information. The whole system can now have only downstream data, but no useful TCP based data transmission will be possible. This attack is mitigated by attenuating the signals from the customers to some degree. If the ingress noise (the kill) exceeds the attenuation limits and decreased the SNR at the CMTS upstream port enough a Denial of Service is noticeable. Only physically detaching the attack-noise will solve the issue. The best solution is to monitor for such incoming noise and to detach those nodes very quickly so that they cannot harm other customers. There exist intelligent monitoring devices (usually to check the amplified signal levels) from vendors like `Kathrein`, or `Triax`. Those devices usually have an SNMP agent and send traps to the monitoring station so that an appropriate action can be taken. The downside of such devices is the requirement of sending upstream data and therefore they may enable other security problems (e.g. cloning, DoS).

4.3.2. Man-in-the-middle attacks

DOCSIS suffers from many layer two and three vulnerabilities, because the protocol adopts many lower and higher ISO/OSI level functionalities. One of the attacks has the goal to receive genuine customer traffic or even to manipulate it. Such attack vectors are now discussed further.

Rogue DHCP server A DOCSIS network forms a layer two network. At the provisioning process of a cable modem a DHCP server is searched by the CM to determine further configuration. A rogue DHCP server may be put into this network by an attacker. This only requires a valid online CM, which is connected to a rogue DHCP server at the CPE side. The DHCP service may offer IP addresses in the known (correct) range or in another. Furthermore, the malicious device may act as the gateway for the attacked CM (and/or the connected CPE) and thus forwards the normal user traffic to the usual gateway (the legitimate CMTS). Therefore, all internet (upstream) traffic can be wire-tapped by the attacker. To mitigate such attacks CMTS rules and proper provisioning process configuration (depending on the features of the CMTS) must be done at the CMTS. The CMTS should only register valid CMs, and CPE DHCP requests by the use of a known trusted DHCP server, which is in the best case directly connected to the CMTS. Due to the fact that all traffic has to go through the CMTS, it should block DHCP messages from regular customer MAC addresses to mitigate such attacks. Moreover, the CM configuration file should already contain a filter for outgoing traffic, so that a wrong DHCP server behind a regular CM will not answer other CMs requests.

Authentication of the CMs At the provisioning process of a cable modem, the CMTS may (depending on the configuration and version) check the CM through certificates. If the CM is a legitimate modem, it is allowed to go online and can proceed with the provisioning steps. The certificate chain is based on a root certificate, which must be installed into the CMTS (it is issued by CableLabs or from the European division). The next hierarchy are the manufacturer certificates, which themselves sign their device certificates. The main problem in connection with these is the one sided check. Only the CMTS checks the CMs certificates, not the other way around. There is no issue for the CMs to come online or another recognition by the users, that the CMTS has not checked their certificate. Furthermore, an attacker may put a malicious CMTS physically before the genuine head-end CMTS. The malicious CMTS may act on the one-hand as a regular cable modem to the legitimate CMTS, but drop, modify or send additional information to the victim (one CM, or even a whole node). The imitating part (CM of the victim) of the attacker device does not usually have the correct certificates for the MAC addresses used, but most cable providers suffer from downgrade attacks (e.g., using only BPI, or even no security measurements). Moreover, it may be possible to steal the private certificate via SNMP or implementation bugs. Of course, this attack is more theoretical, but it shows the doubtful single authentication step done by the CMTS and the misinformation of the customers. A regular user has no clue if his modem is authenticated to a legitimate cable CMTS or if it is connected to a malicious device, which may execute a man-in-the-middle attack.

Data authentication Current security specifications of DOCSIS do not include a feature for (users payload) data authentication. All cryptographic suites are only used without data authentication. The consequence is relevant in the case of leaked traffic encryption keys. If a malicious person can decipher or encrypt in the same manner, so that the cipher- or plaintext do look like as from the legitimate CM (behaves correct), there is no chance at the CMTS do detect this. The CMTS will not check the encrypted payload data integrity or authenticity. There is no additional step for the malicious person to sign or add an integrity field to the data for correctness or authenticity. Of course, this is only valid for normally encrypted user payload data. Some messages, like for the provisioning, have attached a keyed HMAC. [41]

4.3.3. Network attacks

In this section considerations regarding the network architecture are described. The main issue is the correct data flow.

Legitimate data flow One attack vector is the unprotected data flow between the CMTS, the provisioning system and all connected cable modems including the CPE devices. Of course, a provider cannot do much, except blocking bad connections from the CPE devices (e.g., CPE IP range to management IP range), but the CMs and the headend equipment must have access control lists to permit only legitimate data flow. One example is that IP packets must match the right MAC addresses, according to the ones learned during the (hopefully checked and secured) provisioning process. This denies simple attacks, such as statically set IP addresses. Moreover, the modems SNMP interface should only be accessible from the headend's monitoring system.

4.3.4. Insider attacks

Although an attacker can learn plenty about a cable company structure from the outside or as a regular subscriber, he does not know all passive components, which can help to find other vulnerabilities, such as upstream sniffing. One of the most common attacks is cable modem cloning. Basically, an attacker clones the MAC address of someone else [30]. For this task, a MAC address of another node is better suitable, because the chances of getting online are higher. This is due to the fact that many cable companies used one central customer database in the past and the provisioning system did not distinguish between different nodes or cable modem termination systems. The parallel use of the same MAC address work in such cases, because each node (or CMTS) has its own IP range. Therefore, an insider has advantages as the probability of a successful cloned modem attack is much higher, if he knows the CM MAC addresses of other nodes and also the behavior of the customer and provisioning system. [7]

An administrator or operator of the DOCSIS network, which has the ability to create new customers, could also introduce a new imaginary user. This new account can afterwards be used for illegal activities or to give (or sell) it to other cable participants. It will be very hard for the company to detect such issues, because the cable administrators did this intentionally and therefore those accounts might be undetected (or at least until a legal complaint).

An insider attack may also enable the use of multiple cable modems under the same provisioned subscription. The goal is not to impersonate someone else's subscription, it is rather to use or share one subscription with other users (e.g., friends don't need to pay for it). The first phase is to have a second device, with the same MAC address and other parameters (e.g., serial number, manufacturer and general behavior). The next step is to decide the method of operating the two (or possible more devices) to extend the subscription devices. Of course, if the devices are behaving intentionally, each can be exclusively used. The other non-connected devices cannot be used, and thus a timing scheme of operating them must be developed by the malicious persons. Another more sophisticated method is a semi-permanent operation. The downstream link is always broadcasted, therefore each device will receive the same information and only extract the relevant ones. Therefore, the next entity must decide if the data is of relevance (e.g., the CPE device, or the application, which is after the CM). The upstream allocation must be shared by the malicious modems. This can be done by overlaying a time- or counter-based approach (e.g., the second modem uses only each secondary transmit opportunity). Of course, the other CMs do not have to follow cable modem registration when they are powered on, they must rather copy the actual parameters of the original one (SID, configuration file parameters, used encryption mode, etc.). The BPI+ or SEC feature of DOCSIS will prevent this attack, because he do not have the keys and certificates for data encryption and authentication. The insider can leak his private key (e.g. by extracting it out of the CM memory) and the presently used traffic encryption keys to the others (the copied CMs). [6]

Another issue is the execution of the requests for upstream signal opportunities. Only one modem does the solicitation consecutively so that the other modem simple uses the "free" slots to send their upstream data. Of course, to mitigate this attack by a good monitoring system, the signal properties (SNR, micro-reflections, etc.) of each modem must constantly be monitored and changes should be reported.

4.4. Implementation issues

Very often many security issues don't evolve from the architecture of a system. The vulnerabilities are often due to implementation, like the software which is based on a standard. Very often it is only a matter of resources, including time and money to find these bugs in the software.

At the beginning of DOCSIS, some security features of modems and cable modem termination systems were disabled by default in the software or by major cable operators. In some situations, deadlines had to be met, and developers intentionally rolled-out unfinished buggy firmware. Moreover, they wrote about these issues and therefore hackers have a good starting point to exploit them. [30]

This section covers vulnerabilities of headend (CMTS, provisioning system, monitoring) and cable modem (certificate storage, shell, firmware) relevant issues. To reduce the number of insecure and misbehaving devices, DOCSIS developed a certification process, but this process cannot cover all possible issues, and therefore security issues in the firmware will very likely also be found in the future, especially if the CM offers features beyond DOCSIS.

4.4.1. Headend network

The headend covers all devices, which are located on the cable operator side. As the name suggests ,the cable modem termination system is the endpoint for all cable modems and therefore a very critical point. If there is a bug in the CMTS firmware, the whole cable network may be exploitable. The provisioning system is also of interest for attackers, as it is needed to authenticate and authorize the users depending on their subscription.

CMTS DOCSIS very soon implemented a feature to check for altered cable modem configuration files at the CMTS during the provisioning process. The CM must send some of its parameters back to the CMTS, along with a keyed hash, called CMTS MIC (message integrity check). This hash is used by the CMTS to determine an alteration of configuration parameters. The parameter message is encoded as multiple TLV entries. Due to this structure, a configuration file without the CMTS MIC can be generated. One of the first issues of the CMTS was parsing. If there is no CMTS MIC present, the CMTS will not check the MIC, and thus a self-generated configuration file (without CMTS MIC) will always be accepted, and the CM will very likely pass provisioning successfully. [30]

The first version of DOCSIS had no security features to securely authenticate the modems [34]. The consequences in a shared medium are huge. Another person can introduce a cable modem by simply altering the CM RF MAC address. Therefore, the next version included digital certificates to detect CM MAC address alterations, because the modem certificates include the MAC address. Nevertheless, this feature can still be turned off and many CMTS vendors allow self-signed certificates as the default setting [30].

Provisioning system The DOCSIS standard does not specify what an implementation of a provisioning system has to look like, it rather states the needed services and features that are required. It also defines the expiration and retry timers, if one of those steps fails (e.g., because one service of the provisioning system is currently unavailable). The benefit of such a relaxing description is the broad usage of already available software implementations because the provisioning system consists of common daemons, which offer DHCP, TIME and a TFTP service. The bad effect is the (partly) faulty configuration of the features. As seen from the lab environment, a functional and secure configuration of a provisioning system is not easy, and continuously monitoring the connected devices in conjunction with an intrusion detection system (e.g., are the provisioning steps done in the right order and in correct expiration times) is enormously important, but difficult and involves a lot of additional effort.

To mitigate MAC cloning among different nodes the provisioning system (and therefore the services) needs to distinguish and relate customers to specific areas (e.g., node, or even better, also including allowed DOCSIS channels). Most big cable providers in the USA use a central customer database, and the provisioning system just uses this information to serve the appropriate DOCSIS configuration according to their subscription. The parallel use of the same subscription among nodes is not well monitored. This is possible because the provisioning system does not distinguish between nodes (which can be in different cities) and thus the same MAC address can be used in different areas, because they are in different IP ranges and the (in most cases local area or node) provisioning system offers an IP, TIME and sometimes also the configuration file. Of course, it is possible to create scripts or other mechanisms to detect the parallel use of the MAC address, but creating a secure architecture should eliminate such security issues. [7]

4.4.2. Cable Modems

Due to the success of DOCSIS in the cable industry many manufacturers popped up to develop and produce cable modems. The price pressure increased, and providers wanted to offer cheaper internet subscriptions, therefore. The modem prices were decreased too. One of the side effects was the inferior software quality of the devices' firmware. DOCSIS tries to countermeasure this with a certification process so that the major functionality of the cable modems was tested to be compliant according to the standard [30]. This segment describes the most painful and erroneous implementation issues regarding cable modem firmware.

Factory mode Many modem manufacturers (Motorola, Cisco, etc.) include a special mode of their firmware, which is intended to be used in the later stages of the production process. The devices are different from each other because of serial number, MAC addresses and their attached certificates (used for BPI). To set these parameters a

factory mode is included in the firmware. In the case of Motorola (starting from the SB3100 until SB5101) a private SNMP MIB tree is used to change or read those values. Moreover, also directly modifying memory and the execution of code is possible. Another feature of this mode is to update the whole firmware, which can be used to test certain software versions. Of course, the distinct parameters of a cable modem are very important to distinguish the customers, and therefore a change of those values should not be possible by a user. The authors in [30] developed an exploit to enable the factory mode of nearly all Motorola SURFboard DOCSIS 2.0 modems. It uses the normal firmware update mode (set via SNMP) to receive an exploit, which bypasses the firmware update function of the cable modem and overwrites some code to enable the factory SNMP MIB tree. Analog findings and exploits are created for the SB6120 and other Puma5-based devices, which offer similar features like dumping the (private) certificates and managing parameters [7]. For some `Broadcom bcm3380` based devices it is even simpler, it needs only a setting of an SNMP OID to enable the factory mode [87]. Malicious persons are very interested in modems with factory mode enabled, because they may be able to steal the private certificate and can thus impersonate another modem at the BPI+/SEC encryption and authentication step. Most of the firmwares with factory mode feature offer the ability to check the mode by the use of SNMP. Therefore, a malicious person can scan the management network (modem IP range) for factory enabled modems to find victims. [87]

Console and Shell access Early DOCSIS modems had no web-interface to read their status, they rather did offer a simple console port to view their status [30] . Therefore, some modems still offer the possibility to manage the device with a console. Of course, now typical RS232 serial-port or other console accesses are rare, and telnet or SSH management is more and more offered by the modem firmware. For debugging purposes also a shell access is offered by some diagnostic modems (e.g., the `Puma5` reference kit offered by Texas Instruments), or by `General-Instruments` for the `SB2100` [30]. The intended use is to offer technicians more possibilities for troubleshooting problems in the field. Due to the fact that the providers offer more and more services the traditional cable modem is becoming more of a residential gateway with special features (e.g., acting as provider access-point using VPN, DECT station for phones, etc.), also the management of those functionality is done using a shell (typical automated and done entirely from the headend). Of course, this shell can be very powerful. If an attacker can obtain admin privileges he may be able to influence the device behavior and read memory (e.g., private certificates). The attacker might run a virus, worm or other malicious programs (e.g., LuaBot) on it. [88]

Backdoors Backdoors have, from a customer's and technician's point of view, a negative connotation. Of course, it can happen that bad coding leads to unintentional behavior, but backdoors in consumer devices are unacceptable. The vendor Arris has

an undocumented library (`libarris_password.so`) on their modems, which can be used to allow remote logins. Moreover, the firmware uses its own password, which is used to get privileges for special configuration and management features of the device remotely. It relies on a DES-encoded seed (set using a special SNMP MIB entry) to generate the password of the day. Of course, the devices are equipped with a default seed, and many ISPs don't change it. With the use of the password it is possible to activate SSH and telnet services of the device (via custom SNMP MIB or hidden HTTP webpage). Now it is possible to get a restricted technician shell. The even worse thing is that there is another backdoor in this shell, which enables a full `busybox`. This backdoor can also be used by connecting to the activated SSH or telnet service, but another password (based on the serial number) is used. Sadly, the first reaction of the vendor was to the change the backdoor password only, not the solution of the problem itself. [86]

Arris is by far not the only vendor having backdoors in their firmware. At least some CMs from Thomson also have backdoors featuring admin shell access. [81]

To find backdoors and other default passwords in a CM firmware the tools `binwalk` and `foremost` are very helpful. Before analyzing a copy of the software must be obtained. One possibility is to dump the firmware using JTAG or sniffing the connection during an update. The file downloaded during a DOCSIS upgrade is mostly signed (PKCS#7) and compressed, but there also exist only compressed binaries. The first challenge is to uncompress the file (if it is a compressed one), for this task the manufacturer may give lots of insights, as often open-source software is being used, and thus LZMA is a good try. There is a bit of a challenge to unpack it. Due to the fact that some other known software (e.g., very often U-Boot as bootloader) and thus code is in it, there is a high chance of succeeding. Now the unpacked firmware can be analyzed with any program (e.g. AttifyOS[1]). [85]

Certificate storage and access The CM must store and maintain the private and public RSA keys (for the digital certificate during provisioning when BPI+/SEC is enabled) in a secure manner so that disclosure of the private key is restricted and unauthorized access is not possible. Moreover, the device should also limit the access to the important key, so that also in debugging mode no extraction is possible. [41]

Of course, this is not an easy task, because the certificate (private/public RSA key pair) is usually on the same physical storage as the normal firmware. Therefore, security precautions must be done by a vendor to ensure conforming with the DOCSIS specification. The flash is usually partitioned into bootloader, firmware (1 and 2 for updates) and certificate storage, so that during a firmware update the certificate storage is not touched, and the partition is mounted read-only (hopefully).

[1] `https://github.com/adi0x90/attifyos`

Recently the vendor AVM did not put the private key for the device onto the CMs, rather it stored the manufacturer digital certificate (with the private key in it). The firmware can now sign its own device certificate with the stored manufacturer certificate on the fly. Maybe the idea was to have only a single image file for all devices, which can be flashed onto the hardware during production and also if there is a software update, there is no need to take special considerations of the device certificate (with private key). This idea was fatal, as anybody having the manufacturer certificate can sign his own device certificate file for any other cable modem. Of course, this can be used by malicious persons to have legitimate Euro-DOCSIS certificates, because the AVM certificate is signed by CableLabs (or the equivalent for the Euro-DOCSIS). Even worse, an attacker can also use it to impersonate other modems and thus take over another connection. The providers now need to deny the usage of the AVM certificates at their cable modem termination systems (configure the revocation of dubious certificates), and the affected modems must be updated with new certificates (and hopefully a better way of distributing and signing of the private keys certificate). [92]

Of course, there are also other vendors having similar issues. Compal, which is also a vendor of cable modems and mainly used by UPC, also has lots of vulnerabilities in its CH7465LG firmware. The DOCSIS certificate and the private key is stored in the NVRAM area of the device flash chip. An attacker can copy, modify or delete the files either via telnet access, the JTAG or flash interface, or maybe also via a bug in their webserver (which offers remote code execution). A malicious person may impersonate the vulnerable modem, or copy its identity. [24]

Webinterface Many cable modems offer a web interface at `http://192.168.100.1` (at the CPE interface) which shows their status. To access it the PC simply needs also an IP address (netmask `255.255.255.0`) in the same range (usually the CMs expect CPE devices starting at 192.168.100.10). With full access (admin privileges) to the device, special features can very often be activated, like WiFi or VoIP client and DECT features. The DOCSIS standard states a minimal interaction between the modem and the user so that the normal operation cannot be influenced by a customer via the web-interface. However, many modem webpages also offer input functionality, e.g., setting the start frequency or rebooting the device. Of course, inputs increase the attack vector of the cable modems. Therefore, many modems suffer from web-interface based vulnerabilities, some of them are now mentioned in more detail:

- Authentication and defaults: Some modem web-pages are protected and ask for a username and/or password to obtain access to those pages (e.g., Thomson TWG870U, Cisco WebSTARseries). Very often they use default passwords (like admin/admin, admin/password, etc.) because the providers are very often only reselling the device without any modification or consideration. Also the check for authentication may be very insecurely implemented. One device states the valid

login data in the web-page code (which is received by the web-browser), because a javascript checks the input on the fly in the client's browser. Moreover, the login is very probably stored on the flash or on the RAM, so if there is access (via JTAG, telnet, etc.) to those memories, the chances are very high to get the legitimate username and password [30].

- Hiddenweb-pages: The Cisco WebSTAR series modems firmware has many hidden web-pages, which are not visited when logging in as a normal user and following all links. There is also no official documentation of those pages. After some analyzes of the firmware, the asp-files are found, because they need to be physically stored on the flash chip. The special pages are often of interest, because they offer advanced functionality, like setting diagnostic or factory settings. The early DPC modems from Cisco offered a page to update their firmware (via TFTP) without any check of the new one, which is, of course, of high interest for hackers in order to run their own software on those vulnerable devices. [30]

- Web-service implementation: The cable modems contain very confidential information (e.g., private key for DOCSIS encryption, and other factory set parameters). Many cable modems offer a web-interface to access the status or logging information of the device. It is evident that the web-server running on the device must be secure, otherwise malicious persons may crash the modem or have access to confidential and very private data. Therefore, the web service often provides only basic information to an unregistered (logged-out) user, e.g., to see if the modem is successfully provisioned or to reboot it. When valid credentials are given to it, it may offer advanced services, like setting some of the parameters (e.g., start frequency, frequency plan, mode of operation, etc.). A recently published report of the Compal CH7465 modem also revealed many security leaks in its web-service implementation. It uses the `ti_webserver` implementation as basis, which is included in the development kit when designing a Puma5 (Texas Instruments, now Intel) based cable modem, and also offers the service via HTTPS. It is possible to access the private key used by the web-service because the certificate file is not encrypted or passphrase protected. It can be accessed through a normal URL (`http://192.168.0.1/mini_http.pem`), because it was stored in the main root folder, which is served by the webserver. The certificate is self-signed, so usually the user should add it to the trusted root certificates to securely manage the device also remotely via the secure HTTPS connection and also to be safe to be connected to the right device, but because of the extraction of the private key is trivial, a malicious person can generate or even use the same certificate on other devices or impersonate any web site. This vulnerability of the Compal device is not the only security risk, it also offers a remote system command execution. The web-interface offers some network diagnostic features (ping, traceroute, etc.), due to erroneous parsing and other flaws (it also works unauthenticated) application execution with root privileges is possible.[24] Also, other vendors have many security flaws, like

the Arris TG862G, the Cisco DPC3939 and many other cable modems. Those devices had a bug in their webinterface so that arbitrary code could be run. [72]

- CSRF: Even with only the user-feature to reboot the device via its web-interface malicious users can use a cross-site request forgery flaw to disrupt the person's internet service. The first issue is that most Motorola (SURFboard 6141, now most of them are part of Arris) cable modems offer a web-interface using a static, non-changeable IP address. Moreover, the web-interface does not have any authentication. The next problem is the implementation of the reboot feature. Simply requesting the reboot feature web-page executes the reboot. The problem with the implementation is that the reboot-webpage does not check if the user comes from the diagnostic site. Therefore, it is very likely (and proven) that the device is vulnerable to CSRF. A malicious person can simply setup a website with an image (e.g., `<img src="http://192.168.100.1/reset.htm">`). The image source points to the reboot-page of the local modem and the users web-browser simply access it when it tries to download the image. Moreover, the web-interface also offers a second user feature to reset to factory defaults. This feature has the same flaws and thus can also be used by malicious persons to execute this attack based on an embedded image on a webpage to reset the person's modem settings. The consequences are huge: The modem will not only try to reboot, it even resets the frequency database. Therefore, the modem must scan the whole frequency plan, which may take a long time. Therefore, service disruption (DoS) will be encountered by affected subscribers. The best option to mitigate this issue, until a vendor has published an update, is to block access to the site (e.g., block access to port 80 to the IP 192.168.100.1). [59]

- XSS: Most of the web-servers and web-pages implementations do not use (proper) user-input parsing. Therefore, many attacks (e.g., command execution) are possible. The same is true for XSS vulnerabilities. Many cable modems show this weakness. [87]

- Passwords: Even if the DOCSIS standard states considerations about storage and usage of passwords, the real implementations look different. Many times, when a firmware is analyzed with `binwalk` or with other methods, hard-coded and default passwords are encountered. The cable modems can usually be managed via SNMP or telnet/SSH if they offer some very advanced services beyond the DOCSIS features (like residential gateways with WiFi, USB device sharing, etc.). One example of a default hard-coded password in the firmware was reported in CVE-2015-7289. Devices from Arris (DG860A, TG862A, and TG862G devices with firmware TS0703128_100611 through TS0705125D_031115) and Motorola were affected. The devices can be accessed with the known password to manage it via telnet, SSH, SNMP and the web interface. [71]

4.5. Legal aspects

This section describes legal aspects in the context of DOCSIS and especially its security. Often. Legal regulations law has a touch with limitations, but those rules are often useful (e.g., so that the technology can work seamlessly with existing solutions). Sometimes the market and business strategies overrule defined and newly enforced rules. Therefore, it's always good to understand the technology behind it and to get your own picture of the rules that apply. This is especially interesting when signing a cable internet subscription contract; it can be important to understand the limitations of an account and its features besides having a new device sitting somewhere. Due to the rapid speed of the development of the first DOCSIS standard, some security considerations have been neglected (e.g., cloned modems). Some of the security vulnerabilities have also been detected by companies or other institutions, which try to obtain patents for their innovations to close those flaws. DOCSIS was always company driven because the cable operators wanted to compete with the telephone companies, which also offer internet access. Therefore, even the patents have often been submitted by those companies, and therefore only the bigger cable operators benefit from the developed security measures, because they may not allow other companies to obtain a right of use. This can also be seen for the DOCSIS authors, which often work for companies like Cisco or Comcast. In the following technical limitations due to export and law controls will be evaluated; additionally, technical and product obstacles due to patents will be shown.

4.5.1. Technical limitations

Limitations for hardware development often result from different factors, such as protecting the device (e.g., signal power-levels may destroy it), lower manufacturing or operation costs or to sell certain features in another way. [30] One of the first issues while developing DOCSIS was the requirement to use it with already existing and deployed cables. Moreover, it has to work besides the normal use of those cables which broadcasts analog TV signals. Therefore, the FCC (US region) and CENELEC (Europe region) norms and standards must be met regarding signal co-existence. The usable frequencies, modulation, and power levels must be considered. Both analog and other signals of the cable must not be impaired. Therefore, downstream signals (from the CMTS) must use frequency width, distance, and plan regarding the existing NTSC or PAL (depending on the region) signals. The DOCSIS signal should be in the range of -10 dBc to -6 dBc compared to the analog video carriers so that it will normally not exceed any of those levels. The main reason is to mitigate issues with the reception of the traditional broadcasting service because the demodulation and receivers at the subscribers only withstand a certain power level and have a relatively poor segregation of signals. In the upstream path this looks different, because existing norms at that point in time have not exactly considered this. Later on, the FCC and CENELEC specified margins,

frequency divisions (for DS/US), power levels and other considerations (e.g., shielding) not to disturb other services. [40]

The development of DOCSIS is mainly done in the USA and certain features, like the involved cryptography, must follow American law. This becomes very interesting when looking at the used standards and its export rules. The first DOCSIS version had only one data encryption mechanism. It was DES with 56-bit or 40-bit key size. Because of laws, many CMTS manufacturers could only sell devices with DES 40-bit enabled, because of those export limitations. Of course, nowadays most of the export rules do not apply any more to EU and Asia regions [53].

4.5.2. Patents

During the evolution of DOCSIS many providers, companies and vendors developed enhanced features to enrich the standard and make their systems more powerful and secure. Many patents regarding the modulation and the DOCSIS data scheduler have been invented (especially from Cisco). This section describes some interesting patents regarding security improvements to DOCSIS. Many of the patents below are only valid for the US region, and therefore the EU region is not directly affected. The patents restrict a customer from buying DOCSIS hardware from one vendor and may form a monopoly, because of the offered and needed security features which are due to the patents only offered by this vendor.

Method and system for cloned cable modem detection
US Application US7716468
This invention tries to detect a cloned modem, which uses the same MAC address and also keeps the malicious modem from accessing the network. Moreover, the normal operation of the (already) legitimate online modem is not disrupted. The system checks if there is already a modem with a legitimate MAC address online, if this is the case the CM (which has successfully passed all security steps) takes precedence and no further access of the second (cloned) modem is allowed. If the first modem is the malicious device and the second (newly connected) CM is now registering a check is also performed, if the modems differ in the ranging (check if both do answer) and further in their issued security steps (BPI+, DMIC). The idea behind the invention includes a check of the legitimate modem and the malicious modem already at a very early stage in the DOCSIS provisioning (during registration phase). The invention also uses the status of the BPI+ phase and also a dynamic message integrity check (DMIC) to determine the legitimate modem. Moreover, a test is carried out if the two detected modems might be identical. [70]

This approach only works very well when security measures (at least BPI+) is enabled and enforced by the system and also if the clone is not perfect. A very interesting

conflict might arise if two cable modems, with the same MAC addresses show up. The first also has BPI (no certificates) enabled, but it is the malicious modem. The second modem does not perform BPI, when not explicitly enforced (maybe due to a firmware bug). The CMTS is now configured for BPI enabled but does not enforce it (or may not inform the modems to do so). With the invention, the first modem would now be treated as the legitimate modem due to the higher security status (it uses BPI, whereas the second legitimate does not). Of course, this might be a very unrealistic situation nowadays, because newer security measures are available (SEC), but it shows the problems of the algorithm to choose between the legitimate and the cloned modem (some approaches are stated in the invention).

System and method for managing provisioning parameters in a cable network

US Application US20050015810

At the provisioning step in DOCSIS, the TFTP server and CMTS are mainly involved to supply the device with the needed configuration parameters to work and access the cable network. The TFTP server holds configuration files for certain parameter settings. Depending on the needed configuration parameters there might exist a huge number of configuration files because a cable modem can only accept one particular configuration file at a distinct time. For this task, a dynamic TFTP system might be used, which offers the needed configuration file through information from other sources (e.g., based on the requested filename, which encodes some of the parameters). Also, the CMTS may have some distinct provisioning information, a security relevant one is the CMTS MIC, which is used and must be equal to the one used at configuration file creation and thus must be known by a (D)TFTP server. This value must be updated and synchronized. Of course, this is not an easy task in a real environment, because it is done manually and thus human error may occur. Especially when CMs may go online during updating, the MIC is a useless issue (the CMTS might have actually no MIC set and therefore accepts all CM parameters, thus losing the MIC security). The invention provides a system and method for the task of synchronizing parameters from the (D)TFTP server and the CMTS, like the MIC, but also other parameters like service groups or administrative filters are pushed to the cable modem termination systems. Moreover, it is also possible to have a central data-storage, which controls the needed provisioning parameters and pushes those settings to the (D)TFTP server and the CMTSs. Also, changes on a (D)TFTP server can be detected and will be reported back to the central storage (e.g., during monitoring). Now the information can be updated again to the appropriate devices and servers. [28]

4.5.3. Issues and denouncements

Cable modems with a certain chipset and firmware are vulnerable to a denial-of-service attack. The packet processing capabilities of those devices can be overloaded easily and thus users will experience a very poor internet performance because of long delays. The devices are vulnerable via their modem management IP and also via the connected CPE devices IP addresses, which enables the attack to work all over the world. The problem can be triggered via a relatively small amount of network traffic (e.g., 200Kbps), but with a higher number (some thousands) of packets per second spread across various TCP and/or UDP ports. Nearly all Intel Puma 6 chipset-based devices are affected (the firmware is very likely based on the same SDK). This chipset is now used in many DOCSIS 3.0 enhanced (e.g., 32 DS channels) cable modems and therefore many customers are affected by the issue. Major ISPs (e.g., Cox, Comcast, UPC, KabelDeutschland, Virgin Media) use cable modems from different brands with the affected chipset. [16]

The subscribers are very frustrated, because the modems are praised as high-speed gigabit capable devices, but cannot even handle traffic which is a fraction of the claimed traffic speed. One vendor has now been taken to court because of this issue. The modems are told to be defect, because Arris sold the cable modems with quality substantially below the average available market offerings. Moreover, the package indicates they are for high- speed and very fast Internet connectivity which they are used for and therefore are mislabelled. [77]

Now it is getting even worse because also some Puma 5 and Puma 7 chipsets (or rather the firmware) are affected, too. The problem is the degradation of performance when the modems are loaded with a higher load of packets-per-second, regardless if it comes from the WAN/RF (DOCSIS) or the LAN (CPE) side. Texas Instruments sold the cable chipset division to Intel in 2010. It seems that Intel trusted all of the received goods, including software code and had not done a proper quality check on it. Moreover, it is very interesting that the Texas Instruments Puma 5 chipset included an ARM11 processor, whereas the newer Puma 6 and 7 chipsets include Intel's Atom x86 processors. The conclusion now is, that the bug is very likely to be inside the packet-handling (which might be the DOCSIS DSP or something connected to the data handling logic inside the chip). [76]

Chapter 5.

Analysis and evaluation of existing cable networks

Due to the broadcast structure of a cable network, all information from the headend is received at all associated participants. This applies to the normal TV broadcasting services, as well as for the DOCSIS downstream coming from the CMTS. Therefore, each cable socket outlet can be seen as a tap (copy of the information) to that system. The terminology is also used for some of the parts, as a house-connection is usually attached via a tap device output. This device weakens the downstream signals to some degree to keep unwanted ingress noise from the house as low as possible. When internet services were also developed for such broadcasting cable networks the considerations for data privacy and eavesdropping were not that huge. DOCSIS uses encryption to establish data privacy, but this step is mostly done only at the user's data payload. Therefore, much interesting information can still be intercepted as there is no mechanism in DOCSIS to protect the meta information and lots of registration and provisioning data. This chapter gives an overview of data which can be sniffed, how to extract useful information and how an attacker or other people can use them. A system for eavesdropping and data-decoding is introduced. Moreover, some real cable providers are evaluated. The results of the sniffing method and an overall image of the providers-security regarding DOCSIS are presented. All of the information has been obtained passively.

5.1. Information Intercept

This section gives an overview of the downstream interceptable information. Moreover, it is illustrated how this data could be used, because it could be useful for an attacker or malicious person to obtain confidential information. The encryption of data is usually performed for a MAC frames payload. Depending on the encryption it might be possible to decipher it. The lists below give an overview over the DOCSIS data information which is usually transferred in clear-text, even if DOCSIS security is applied or enforced.

The following list shows the usually interceptable CMTS information:

- CMTS IP and MAC address: The CMTS MAC is in nearly all PDUs present, because there is usually much traffic and nearly all of the data will pass the CMTS. This depends if a routed, or bridge CMTS is used, nowadays mostly all CMTS are routed-types and therefore the first gateway for a CM accessing the internet is the CMTS.
- IP version support: The CMTS tells provisioning CMs if it is capable of IPv4 or IPv6 support. Usually IPv4 is used, but the provisioning TFTP, TIME and SNMP server might (also) be accessed through IPv6 addresses.
- Upstream-Channels: Each DOCSIS downstream contains associated upstream channels, which include the frequency, modulation, symbol rate and ID for each upstream.
- RNG (Ranging) messages: The CMTS sends periodic CM adjustments (e.g., frequency, downstream channel, upstream channel, power level, frequency offset) to the CMs. The sniffer may obtain other (to him yet unknown) downstream and upstream channels with their according parameters (e.g., bandwidth, modulation, etc.).
- CMTS EAE Support: A newly registering CM must or can use EAE when performing provisioning. This is very interesting for a sniffer in order to find out if there are chances to capture configuration files and other CM data or if that information is encrypted.
- CMs registration/provisioning status: Whether a CM can access the network is sent by the CMTS during the last step of provisioning. This information is interesting for an attacker to see if a malicious device is successfully connected to the DOCSIS cable network or not.

Additionally to the above mentioned informations also interesting customer devices are detectable. The CM or CPE device usually exchanges periodical information (e.g. CM does periodically station maintenance) or user data (e.g. CPE ARP, CPE application traffic), which the sniffer can capture. The following list is the usually interceptable CM and CPE information:

- CMs MAC address: Very useful for basic cloning attacks. If no additional measures are done at the CMTS, a malicious user may use this sniffed information to impersonate someone else's CM and use the subscription. Moreover, the information can be used for ARP Spoofing attacks.
- CPEs MAC addresses: The devices attached to the CMs are also in a relatively big broadcast domain. Therefore, chances are high to get many CPE MAC addresses. A malicious person may use this information to impersonate someone else's CPE device. Usually, only the CPE IPs are public and routable, therefore, an attacker also wants those MAC addresses to access the internet. Moreover, some providers

associate the CPE MAC to a subscriber account and not the CM MAC (because the CM may have much higher traffic, due to SNMP and other management traffic).

- CM's IP addresses: A CM must have one management IP, e.g., for SNMP access, and may have one or more for other services, like telephony. The IP address is assigned via DHCP to the device during provisioning. If EAE is not enabled this step can be sniffed and therefore also the CM's IP address. Moreover, residential gateways are getting more and more popular now. They are basically CMs with routers and some additional services (e.g., printer sharing) in one case and therefore may also have a routable public IP for internet subscription (Router WAN IP). A malicious person may also use the IP (impersonate someone else and subscription), and some providers tie the user's subscription to the IP (not the MAC or better the digital certificate of the CM).
- CPE IP addresses: Sniffable if no data encryption (BPI) is performed or if ARP traffic is transferred. There also exists a chance to sniff the CPE IP address during the DHCP request/response if a CM needs much time enabling BPI (e.g., when it's not mandatory, but enabled and EAE is not performed).
- CMs configuration: If EAE is not applied at the CMs or not offered by the CMTS, chances are very high to intercept cable modem configuration files. The file contains much information, such as the bandwidth of the subscriber, or the SNMP community string to access the CM agent. The drawback is that this file is only transferred during the provisioning phase of a starting CM. Therefore, the intercepting may take some time until capturing such configuration files or requires an active attack.
- CMs DOCSIS Version and Privacy Support: BPKM-Replies also include performed DOCSIS registration, provisioning and privacy feature support. This might not be the full available list because the CMs support is transferred in the upstream. However, the CMTS replies with the actually chosen features. This information might be useful to make better clones of modems (e.g., use only DOCSIS 2.0, which also means at best BPI+ is possible). Especially interesting is the privacy support, which tells an attacker the used encryption algorithm (DES or AES) for a particular CM.
- Encrypted traffic encryption keys and IV: A CM which performs BPI(+) gets two keys and an initialization vector for data encryption (one for the first time slot, the second for the future until a new key is obtained). This information can be decoded out of the BPKM-Reply messages. It might be useful to know how long the device might be online (e.g., if the key expires and there is no further BPKM-Reply the CM is very probably offline, and an attacker might get online with a cloned modem). Moreover, it is sometimes possible to decipher the encryption key [97], which means the traffic can also be deciphered.

- CM's TFTP server IP: If EAE is not enabled, the TFTP servers IP address, containing the CM's configuration can be sniffed in the DHCP offer. This might be useful for an attacker to download available configuration files or request (on a cloned or hacked modem) another configuration from the valid TFTP server (e.g., the configuration files will probably have the same pass-phrase for the MIC as the CMTS expects).

Moreover, some meta information can be extracted and evaluated:

- Downstream-Channels: The sniffer must first detect the DOCSIS downstream channels. It is possible to go through each frequency according to the frequency plan or to search for it consecutively (e.g., check if there is a signal on each frequency, which takes very long). The modems usually also use the normal frequency plan (e.g., Europe, US or Japan plan) and therefore a normal frequency plan scan is enough to make a listing of all available signals. Now, the applied modulation schema (e.g., 64-QAM, 256-QAM) and symbol-rate (usually 6.952 Msym/s for EuroDOCSIS) are used. This must be intrinsically done or viewed from an modem already online (e.g., the web-interface). Moreover, the information must be checked if it's really a DOCSIS channels (e.g., it contains the MPEG 2 transport stream with PID 0x1FFE).
- CMTS periodically sends many RNG (ranging) messages for a particular CM: Indicates a problem with a cable modem (mostly in the upstream path).
- Suspicious applications: Detection of IP scans (Usually high ARP traffic) and virus programs or other programs which consume much traffic (botnets)
- Utilization: Currently used bandwidth, is over-utilization happening (especially interesting if poor speed is encountered)

Which DOCSIS PDU actually contains the mentioned information is evaluated in detail in the section "practical cases", which can be found in the results section, because some of the information heavily depends on the CMTS configuration, the provider network and other devices (e.g., firewall, CM software).

5.2. Sniffing System Method and Considerations

The sniffing system consists of a hardware part, which captures the signals, and a software part, which decodes and analyzes information. The capturing device must somehow provide the information of certain frequencies to the software. The signal receiver is connected to a cable outlet (free or disconnected from a device), to a tap output or a splitter. Which hardware parts are used and special signal properties to consider are stated now. Moreover, the software part is described.

5.2.1. Signal Filters

One consideration is the usage of filters. Some providers (especially in the past) used filters to block certain services. When DOCSIS got deployed, usually a higher frequency was used for the internet service and in order to minimize system ingress (from other devices like TV sets, which are no cable modems) band-stop filters sometimes got installed for TV-only subscribers or outlets. Nowadays it is very likely that all downstream signals are on a TV-cable socket, as the DOCSIS channels may be spread around all free, available frequencies.

5.2.2. Sniffing Detection

Another deliberation for a sniffer is the detection possibility by a cable operator. The eavesdropping hardware is nearly identical to a normal TV receiver circuit, which means electrically it is remotely impossible to tell if the device is a DVB-C tuner or the sniffing hardware. The problem may begin when the contract is signed for a certain number of cable outlets and no additional splitting is allowed. However, usually this is not the case and nowadays the providers allow to attach CENELEC conform devices. Mostly, providers care about it when the services may be negatively influenced. This might be the case when (high) ingress is coming from a subscriber or from any other connected cable. Therefore, it is a good idea to attach a filter device (e.g., frequency band blocker and/or good splitters with high isolation) between the sniffing hardware and the attached cable socket. This minimizes unwanted signals from the tuner or any other circuitry from reflecting signals back into the provider cable network. A disconnected cable socket is mostly worse, because of the reception of other signals and reflecting them into the cable plant, than a proper tuner of a sniffing hardware, as it will have a defined termination (75 Ohms) at the cable outlet.

5.2.3. Hardware

The hardware for the case study consists of a traditional PC (details can be found in the appendix), a USB DVB-T/T2/C stick, and an antenna cable to connect to a free cable TV socket. The PC needs to reassemble all 188-byte long MPEG TS packets to one data stream and extract the DOCSIS PDUs later on. Furthermore, the analysis of the payload of the DOCSIS data is done at the PC. The sniffing device is a very cheap cable TV receiver for PCs and will be used as normal DVB-C receiver. Of course, also other SDR devices can be used, but they need to provide the needed bandwidth (8MHz for EuroDOCSIS 256-QAM downstream channel). The USB DVB receiver is called *Astrometa DVB-T2* and consists of the following components:

- Realtek RTL2832P: Chip containing a high-performance demodulator, connected to an external demodulator and a USB 2.0 interface
- Panasonic MN88473: DVB-T/T2/C demodulator connected to the RTL2832P and controlled via I2C
- Rafael Micro R828D: RF tuner, connected to the MN88473 demodulator and the RTL2832P demodulator, also controlled via I2C

One issue with this setup is that only one DOCSIS downstream channel can be captured at a particular time. This might be a problem when channel bonding is performed, because DOCSIS packets are transferred concurrently on different channels to get an overall higher bandwidth. Depending on the number of bonded channels the same number of DVB-C sticks will be needed (or another SDR with as many tuners and demodulators as the bonding number in the DOCSIS MDDs). Nevertheless, most of the interesting information is not spread across the channels, and this case study is more interested in the management DOCSIS PDUs (which are mostly not spread), not in the actually transferred subscriber data payload.

5.2.4. Software

The software part of the sniffing system must basically do the same as a cable modem (only downstream), which is the reception of the MPEG TS datastream from the demodulator (DVB-C-stick), the filtering of the PID, reassembling of the DOCSIS stream from the MPEG transport stream, extracting and reassembling the DOCSIS PDUs (which might be spread across different channels). The last step is the extraction of interesting information (e.g., MAC addresses, IPs) out of DOCSIS data. The PC runs Ubuntu 16.10 (x64) as operating system (Linux kernel 4.8.0-59-generic). The next step is to compile the driver for the USB DVB-C receiver and to install the software for data reception and analyzing.

Driver for DVB device

The Linux kernel already includes a driver for this device, but it is very buggy. The MN88473 DVB-C demodulator talks with the main chip via I2C, but there is a lot more going on over this bus (e.g., infrared reception of remote control signals). Therefore, a fix is to make the I2C bus faster and to avoid some EMI issues [80]. Moreover, the stick also needs a firmware (needs to be downloaded from [1] and placed into `/lib/firmware`), which is downloaded to the main chip when powering and connecting to the PC via USB. The patch to solve the I2C issue is very simple. It sets the RC (remote control receiver via I2C) polling time lower, maybe this reduces the risk of other data sent at undesired

[1] `http://palosaari.fi/linux/v4l-dvb/firmware/MN88473/01/latest/`

times [56] too avoid corrupted data at the bus. There is a git repository [2] with the fixed version available, how to build in the driver is shown in the appendix. Now the DVB-C USB receiver works well and the sniffing of DOCSIS downstream channels can be started.

w_scan

The tool w_scan[3] is a utility to scan a certain frequency range for TV (DVB, ATSC) channels. The purpose of this tool is to find frequencies which transmit MPEG TS data. It also reports the PID and, therefore, can be used to search for DOCSIS channels, which will report a PID of `0x1FFE`. The program can be started using this: `w_scan -f c` (Option `-f c` is important to use the DVB-C demodulator). It will try the first found tuner and frontend (important if more DVB-C receivers are connected). Moreover, the mentioned command searches for EuroDOCSIS channels, as DOCSIS channels will very likely use NTSC and therefore an ATSC TV receiver must be used. The output must be searched to determine the possible DOCSIS downstream channels.

dvbtune

If a valid DOCSIS frequency channel is found the tool `dvbtune`[4] can be used to tell the RF tuner to receive signals at this frequency. The following command can be used to do so: `dvbtune -f downstream-frequency -s 6952 -qam 256`. The `downstream-frequency` is the exact channel frequency given in Hz and the `qam` option depends on the used modulation, reported by `w_scan` (usually 256-QAM).

dvbsnoop

When the RF tuner is tuned to a valid frequency and locked to it (e.g., has a good signal reception) the data can be received with the tool `dvbsnoop`[5]. The program can be used to view, debug, dump and store the stream data. It can do this live or use an already saved file. The following command can be used to capture the traffic of the DOCSIS PID (the adapter must be first tuned and locked to the chosen frequency, e.g., with `dvbtune`: `dvbsnoop -s ts -frontend 1 -adapter 0 0x1ffe > docsis.stream`. It is also possible to capture the whole TS stream with the additional `-tsraw` option and omitting the PID. The tool can also be used to store a defined amount of data (e.g., stop until some seconds or after receiving a defined data amount). Moreover, the tool can also be used to get some statistics about the utilized bandwidth of a particular

[2] `git://linuxtv.org/anttip/media_tree.gitastrometa`
[3] `https://linuxtv.org/wiki/index.php/W_scan`
[4] `https://www.linuxtv.org/wiki/index.php/Dvbtune`
[5] `http://dvbsnoop.sourceforge.net/`

DOCSIS downstream channel: `dvbsnoop -s bandwidth`. Optionally a PID can be set to get the raw DOCSIS bandwidth only (because there might be other PIDs in the MPEG transport stream, but this is very unlikely).

packet-o-matic (pom-ng)

Packet-o-matic is a live network forensics tool. It can parse simultaneously from different inputs (e.g., DVB cards, files, network interfaces). Moreover, it processes the information according to rules. The program also detects the protocol, and it's headers inside of the inputs and further analyzes and reassembles the information. It also keeps track of packets related to connections. Also, events can be specified and will be generated for higher-level protocols (e.g., an application, like HTTP will execute events for a GET request of a website and a response if received in the input data). The events also include the payload data, which is in the case of an HTTP response the returned HTML code. Also, there exist some payload analyzers, which for example report the width and height of JPEG-images inside of a returned and captured HTML website. Moreover, the program can store everything in multiple outputs, which can be a raw-file (or pcap-file), a network interface, or an event file. The tool can be controlled via a CLI or via a web-interface, which is quite nice. [63]

DOCSIS sniffing, processing and analyzing The program `pom-ng` also has an input plugin to search for valid DOCSIS channels. This is very handy to get a list of downstream channels. Moreover, the plugin states if a found DOCSIS channel is primary capable (e.g., contains SYNC, MAP, and UCD packets). It also has a feature to automatically add the found DOCSIS channels as input to `pom-ng` with the correct settings. Of course, it is also possible to add a DOCSIS channel manually as input. It is also possible to sniff the DOCSIS channel via the DVB-C or ATSC API, which means it has to go through more layers (e.g., it needs to filter the PID in software, whereas docsis-input uses hardware filtering) and therefore tends to be slower. With one DVB-C receiver it is only possible to sniff one channel at a particular time. So, it filters traffic which is sent across multiple channels because the result would otherwise be unsatisfying (e.g., corrupted packets cuase significant load because pom-ng tries to assemble them and due to TCP and other protocols this will consume a large amount of resources). However, this filter can also be turned off, to get the all received DOCSIS data (including garbage). If more DOCSIS inputs (more DVB-C cards) are available and connected, it makes sense to set the filter (`filter_split_traffic`) off, because the sniffing can be done on all channels in parallel and, therefore, `pom-ng` will re-assemble all DOCSIS data. [64]

The output can now be saved to a file or directly analyzed by protocol analyzers, some of them are already included in the web-interface. They offer the ability to follow HTTP

connections and store the found images, or search for received passwords in plain-text. Moreover, they include a graphical representation of the traffic. The output can also be a virtual network interface (`tap` device). This is very handy as the network device can be captured and analyzed with other tools, like `Wireshark`[6] or `tcpdump`[7].

5.3. Analysis

This section shows the results of the received and decoded DOCSIS information from real cable networks. All of the extracted information can, in theory, also be received via a digital TV-tuner. The DOCSIS channels of the networks are found using the program `pom-ng` with the `docsis_scan` input plugin. Moreover, the DOCSIS and provider data is used to determine and draw conclusions about the security of the network. Possible vulnerabilities and attacks are mentioned. Some of the results are obfuscated (e.g., most public IPs, overwritten with `X`) to keep the privacy of the providers.

5.3.1. Provider I

This provider is relatively big (compared to others in Austria, but small compared to Comcast). It offers products from internet speeds starting at 16/1 up to 250/25 Mbit/s. Moreover, there are also telephony and WiFi enabled residential gateways available. The provider sells dedicated lines, wireless products and, of course, cable-based internet subscriptions.

5.3.1.1. Results

The first step to do further analyzes is to find the DOCSIS channels. After plugging and attaching the TV cable to the stick and the stick to the PC, the program `pom-ng` was started and the input `dvb_scan` was added. Unfortunately its configuration had to be changed, as the DVB-C receiver frontend for cable is `1` (`pom-ng` defaults to 0). After changing this setting and starting the scan it took a while to find the channels, which can be seen in in figure 5.1:

[6] `https://www.wireshark.org/`
[7] `http://www.tcpdump.org/`

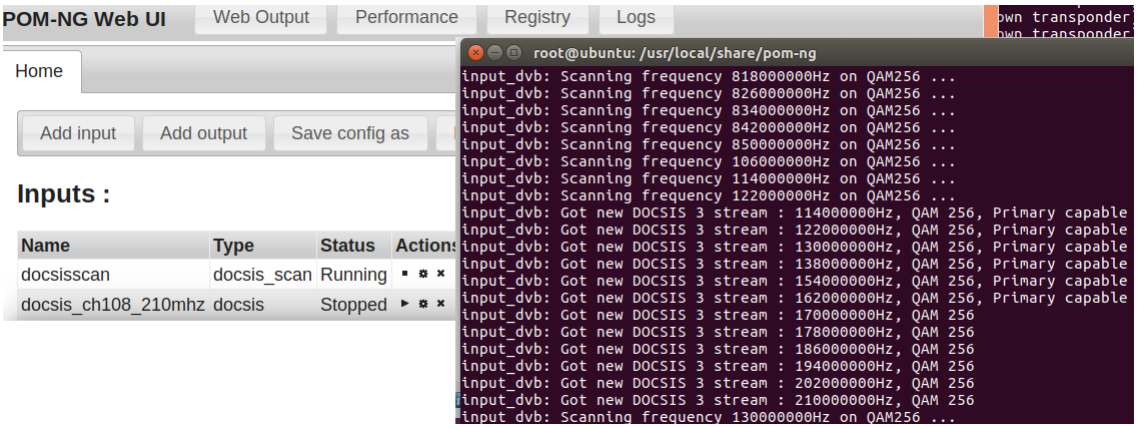


Figure 5.1.: Found DOCSIS channels for provider I using `pom-ng`

Thankfully, `pom-ng` added all the found channels, so the input could be easily started and stopped. The found channels are automatically named according to the channel ID sent (set at CMTS DOCSIS port, usually corresponds to the local frequency plan channel number). A modem can only provision on a primary capable channel (contains DOCSIS SYNC, MDD and UCD messages), therefore this information is also useful, because chances are high that those channels also contain BPKM messages. There are overall 12 channels (6 primary capable). Due to having only one tuner the analysis is limited to going through each channel consecutively. This means that bonded data might be incomplete (the filter for bonded data is turned off, to get as much information as possible). Due to the massive amount of packets and data the sniffing of each channels was limited to some minutes (each channels could have up to 50 Mbit/s of data throughput).

Type	Packets count	Packets compared
BPI(+) enabled	3174481	99.97%
BPI(+) disabled	967	0.03%
EAE enabled	1	0.09%
EAE disabled	1055	99.91%

Table 5.1.: BPI(+) and EAE statistics

Security parameters Table 5.1 shows BPI(+) enabled DOCSIS packets and EAE-enabled MDDs. The BPI enable attribute is in the DOCSIS header field and the EAE feature is in the MDD messages. It can be clearly seen that BPI(+) is turned on and nearly all CMs have established it. Nevertheless, there are some packets which do not have BPI enabled, which means that it is optional to do, or there is an exception for

certain CMs or Service-Flows. Early authentication and encryption is not enforced, nor does the majority of the CMs. Unfortunately, there is one packet with EAE enabled. This can be due to a test or it may also be a damaged captured packet (e.g., bad SNR perhaps). Moreover, no DOCSIS configuration file could be captured, which might be possible if a longer sniff is done. One BPKM response was captured, it includes the encrypted TEKs, IVs and their lifetime (22199 seconds). Moreover, the response defines the key length of 56 bit, which means the DES cipher algorithm is used (at least for the particular SAID, very probably for the whole CM, but this can only be stated if the configuration file or all dynamic flows are known).

Network statistics Apart from the security parameters, some interesting network addresses are discovered. The count of unique MAC addresses is `7311`. This includes CPE, CM and CMTS MAC addresses. A small CMTS usually has one MAC address, but it is also possible that each DOCSIS channel has it's own MAC address. The CMTS of this provider seems to have two MAC addresses. This means that the CMTS very probably has two big line-cards (or those two are connected to the segment were the sniffing is done) and those are very probably in a cable bundle, because the connection statistics of `Wireshark` detected only one IP address with major traffic, which is very probably the CMTS bundle IP). To determine if it's a CPE or CM MAC address the previously sent registration and DHCP messages would be interesting, but it may also be possible to distinguish these groups because of their IP addresses (and they can be related to the MACs e.g via ARP or DHCP traffic). Another approach is to lookup the manufacturer and probably the device via a MAC address to vendor table (e.g., if the lookup points to vendor Arris it is very probably a CM). The CMTS has the MAC address `X:13:7f:31:af:aa` (captured from DOCSIS SYNC messages). Its IP address is very probably `10.202.0.1`, which can be determined from the DHCP messages (relay agent, message is not encrypted) and other payload traffic. The DHCP-Server has the IP `172.16.100.153`. The received DHCP messages also include the client's IP address (usually in the `X.217.50-63.Y` range), mask (/24) and DNS servers (`X.202.138.3, X.202.128.3, X.40.128.2`), gateway (`X.217.48.1`) for the CPEs and the CMTS second IP for CPE traffic is `X.202.0.1` (public IP), which is determined from DHCP ACKs (relay agent). Moreover, using the connection statistics of `Wireshark` 54 unique IPv4 addresses, 97 TCP connections and 8 UDP data packets are detected, which relates to the fact of some cable modems not encrypting the frames payload. During the capture 112 dynamic service change responses were reported, most of them were initiated by the CMTS and, therefore, it is very likely that VoIP/telephony calls were established or terminated. Another interesting detected protocol is STP. It might be used to prevent broadcast-loops from happening if two cable modems are directly connected to each other (CPE to CPE interface of the CMs) to the DOCSIS cable network segment. Moreover, some WiMax protocol packets are sniffed. The provider

also offers wireless internet subscription, which may use WiMax and thus they might use the DOCSIS network to bridge the connection to the stations.

Meta information The provider network offers 12 channels for DOCSIS downstream data. Moreover, they are DOCSIS 3.0 (and downwards) compatible and channel bonding is enabled for the lower half of the channels. If concurrently used, a maximum bandwidth of roughly a speed of 600 Mbit/s is available in the downstream for that particular node, which means that the provider will probably overbook the shared media. The utilization during the case study can be determined from the capture time (5046 seconds) and the received amount of data (5.507.712.524 Bytes). This gives an average throughput of 8.73 Mbit/s (max. is 50 Mbit/s), which equals about 17.46% of utilization during the capture. This relates to the fact of not over-booking the media too much, as there is plenty of free throughput for rush hours or peaks of throughput. The CMTS announces 8 available upstream channels through the UCD messages. They also offer bonding capabilities and use 16-QAM modulation with a bandwidth of 3.2 MHz. This means, each channel offers at about 10.24 Mbit/s (8.9 Mbit/s usable) and overall 81.92 Mbit/s (71.2 Mbit/s). Of course, this is a little worse compared to the over-booking of the downstream, but usually the upstream is shared with less cable modems compared to the downstreams.

5.3.2. Provider II

The second provider is a much smaller one (compared to the first) and has between 1000 and 5000 subscribers. The product range is from cable-TV, cable-telephony, DSL, up to wireless subscriptions. The data rates for cable subscriptions are 16/3 up to 100/10 Mbit/s (DS/US).

5.3.2.1. Results

Analogous to the first analysis the DOCSIS channels must be found. The tuner is connected to a regular TV socket. This provider has 8 downstream channels (ID 49 to 56), the first four are primary capable. Like in the first case, `pom-ng` automatically successfully added the channels if found as inputs to perform further analysis on the signals.

Security parameters During the capture time of over 30 minutes no encrypted (BPI+ enabled) DOCSIS packets were received. Therefore, the CMTS is not securely authenticating the CMs nor is there any encryption of the DOCSIS payload data. Of course, this is a bad situation, malicious people can sniff and read all traffic, if it is not encrypted at higher OSI levels. it is possible to do further analyzes (e.g. received

passwords, HTTP connections, FTP etc.). The provider also does not check certain parameters of the CMs via SNMP and therefore it is very likely that the provisioning, authentication and accounting is based on the MAC addresses only. Those can be easily faked and an attacker can impersonate another CM and/or CPE.

Network statistics During the provider analysis `2840` unique MAC addresses and `3579` IP addresses were discovered. Because of the unencrypted data flow, `26294` TCP and `8903` UDP connections were determined. Of course, it only depends on time to differentiate between the CPE and CM addresses and methods mentioned for the previous provider can be applied (ARP, or DHCP). Many of the CMTS and provisioning system addresses can be found inside the received DHCP and SNMP messages, especially the CM relevant provisioning information can be found in figure 5.2. The CMTS MAC is `X:d3:f1:80:de:60` and it's IP is `X.255.145-159.1`, the GW for CMs and CPEs is `X.255.156.1`. The DNS servers are `X.255.144.75` and `X.96.0.4`. Moreover, the IP of the TFTP, TIME, SYSLOG, SNMP monitoring and DHCP server is `192.0.0.11`.

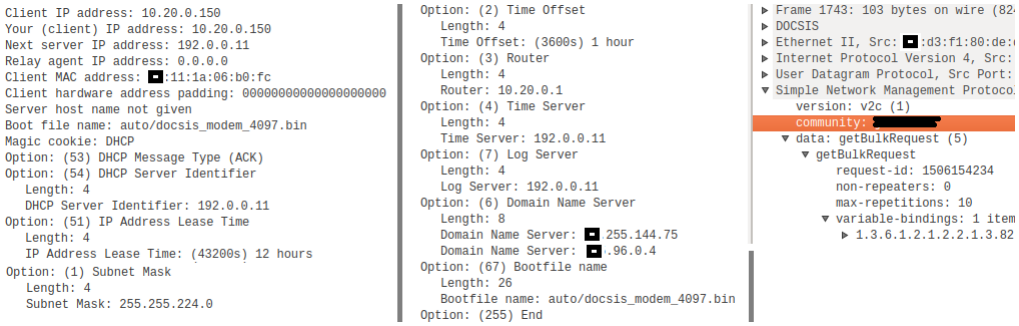


Figure 5.2.: Received DHCP message for CM (left and middle) and SNMP get request (right)

In figure 5.2 is also a SNMP get request from the monitoring agent in the headend to a CM. Furthermore, this SNMP data is consecutively sent to all CMs. Moreover, this action is periodically done every 5 minutes. The monitoring station wants to get the information about SNR and other statistics of the modem, probably to monitor for signal issues. Another very interesting fact is the stated SNMPv2c version, which means no protocol encryption is done nor (secure) authentication and the community string to have access to the CMs agent is stated in their DOCSIS configuration files. This makes it easier for attackers to gain access to a modem because of the CM configuration file a monitoring station access must come from the headend IPs, but they may be spoofed.

CM configuration file During the case study a new cable modem registered on the cable network and was provisioned. The most interesting settings are found in listing

5.1 and will be discussed now. One complete CM provisioning was captured and the file `auto/docsis_modem_4097.bin` was transferred during the analysis. This makes it possible to understand nearly all of the DOCSIS parameters, which the particular CM got in it's configuration. The fully (anonymized) decoded configuration file can be found in the appendix. The textual representation gives insights into a particular CM's parameters:

```
1  SNMP MIB Object(docsDevNmAccessIp.1):1.3.6.1.2..., IP Address, X.255.144.0
2  SNMP MIB Object(docsDevNmAccessIpMask.1):1.3.6.1...., IP Address, 255.255.255.128
3  SNMP MIB Object(docsDevNmAccessCommunity.1):1.3.6.1..., Octet String, ------
4  ...more SNMP entries, to allow 192.0.0.11...
5  Maximum Number of CPEs:2
6  Upstream Packet Classification Encoding
7    Classifier Reference:1
8    Service Flow Reference:2
9    Rule Priority:50
10   Classifier Activation State:on
11   IP Packet Classification Encodings
12     IP Protocol:256
13     IP Source Address:10.0.0.0
14     IP Source Mask:255.255.0.0
15 ...many more packet classifiers for X.13.26-30.0 (probably VoIP/telephony)...
16 Upstream Service Flow Encodings
17   Service Flow Reference:1
18   Service Class Name:ucountme
19   Quality of Service Parameter Set:provisioned admitted active
20   Traffic Priority:3
21   Upstream Maximum Sustained Traffic Rate:1000000
22 ...more upstream service flows...
23 Downstream Service Flow Encodings
24   Service Flow Reference:11
25   Service Class Name:dcountme
26   Quality of Service Parameter Set:provisioned admitted active
27   Traffic Priority:3
28   Downstream Maximum Sustained Traffic Rate:15500000
29 ...more downstream service flows for the classifiers...
30 Privacy Enable:off
```

Listing 5.1: Decoded received CM configuration file (auto/docsis_modem_4097.bin)

The first entry restricts the cable modems SNMP agent to only accept access from the provider headend (X.255.144.0/25) and from 192.0.0.11 (omitted). Moreover, 2 CPEs are allowed, this means two PC's (two different MAC addresses) can be connected to the cable modem at a particular time. There is an upstream packet classifier defined, very probably for telephony (data will not count as normal traffic, data priority). The classifier is activated in the upstream direction for data packets destined to 10.0.0.0/16.

Moreover, a downstream service flow is defined analogous to the upstream one. Both classifiers have a maximum traffic rate stated (which is very likely the rates of the subscription) and a service class name (`ucountme, dcountme`), which may be used to count the traffic at the CMTS. Moreover, there is a priority of 3 defined, which schedules the traffic to middle priority. The VoIP traffic classifier also has the same priority, which means congestions due to overbooking of normal user data traffic will very likely badly influence the telephony traffic. Additional to the mentioned classifiers and service flows there are more entries for another IP address (probably also telephony or backup services) defined. All DOCSIS privacy features are turned off at the last line in the configuration file.

Other CM configuration files During the passive sniffing of the DOCSIS downstream channels some more interesting CM configuration files got transmitted.

```
1  Downstream Frequency Configuration:506000000
2  Network Access Control:on
3  ...SNMP MIB Objects to allow only SNMP access from headend...
4  SNMP MIB Object(OID 1.3.6.1.4.1.2863.205.10.1.10.1.0):Integer, 1
5  SNMP MIB Object(OID 1.3.6.1.4.1.2863.205.10.1.10.2.0):Integer, 1
6  SNMP MIB Object(OID 1.3.6.1.4.1.2863.205.10.1.10.3.0):Octet String, -(omitted)-
7  SNMP MIB Object(OID 1.3.6.1.4.1.2863.205.10.1.10.4.0):Integer, 1
8  SNMP MIB Object(OID 1.3.6.1.4.1.2863.205.10.1.10.8.0):IP Address, X.255.151.8
9  SNMP MIB Object(OID 1.3.6.1.4.1.2863.205.10.1.10.9.0):IP Address, 255.255.255.248
10 SNMP MIB Object(OID 1.3.6.1.4.1.2863.205.10.1.10.10.0):IP Address, X.255.151.9
11 SNMP MIB Object(OID 1.3.6.1.4.1.2863.205.10.1.10.11.0):Integer, 2
12 SNMP MIB Object(OID 1.3.6.1.4.1.2863.205.10.1.10.12.0):Integer, 2
13 SNMP MIB Object(OID 1.3.6.1.4.1.2863.205.10.1.10.99.0):Integer, 1
14 ...Classifiers and Service Flow Encodings (omitted)...
```

Listing 5.2: Second received CM configuration file

The next one can be found in listing 5.2. It includes a statically set downstream frequency (506 MHz), which means that the CM can only register on the particular downstream channel. If it downloads the configuration file via another DOCSIS DS channel it must reinitialize its tuner with the stated frequency. Moreover, it includes some special SNMP OIDs. Those are not part of the DOCSIS specification, but a manufacturer could enrich the CMs functionality using their private or public SNMP OID tree. The stated settings activate the CM's routing protocol feature (RIPv2). It also states the settings of the RIPv2 engine, especially the password (OID 1.3.6.1.4.1.2863.205.10.1.10.3.0). An attacker might run his own RIP instance and maybe route the traffic via his gateway to sniff the traffic. The usage of a password is also no real security gain, because the password is stated in the (decode-able) configuration file and it must be the same for the other remote RIPv2 instance at the provider location.

The third received CM configuration file was called `FLAT-Thoms_Tel_WL-off.cfg`. As the name suggests, the file includes settings for the SIP MTA feature of the CM and the WiFi is turned off.

```
1  Network Access Control:on
2  ...SNMP MIB Objects for agent settings...
3  SNMP MIB Object(OID 1.3.6.1.4.1.4413.2.2.2.1.18.1.1.2.1.12.32): Integer, 2
4  SNMP MIB Object(OID 1.3.6.1.4.1.4413.2.2.2.1.18.1.1.1.0): Integer, 1
5  Maximum Number of CPEs:5
6  Upstream Packet Classification Encoding
7    Classifier Reference:1
8    Service Flow Reference:2
9    Rule Priority:100
10   Classifier Activation State:on
11   IP Packet Classification Encodings
12     IP Protocol:256
13     IP Source Address:X.13.40.0
14     IP Source Mask:255.255.255.128
15 ...more Classifiers and Service Flows, probably for telephony and management...
16 Privacy Enable:off
17 Euro-DOCSIS vendor specific Extension Field:001095/190... (telephony feature)
```

Listing 5.3: Received CM configuration file (FLAT-Thoms_Tel_WL-off.cfg)

Listing 5.3 shows the interesting settings, which differ from the other received CM files. Of course, the configuration includes settings for the SNMP agent to be only reachable from the headend IP range. Moreover, it also deactivates the DOCSIS privacy features (encryption, etc.). There are two special SNMP OID settings, which set the WiFi functionality of the cable modem to off (vendor dependent, the CM is very likely a residential gateway and includes a router). The file also includes a (Euro-)DOCSIS vendor specific extension field. This can be used to tell the CM to activate or set special features of the device. In this case it is used to enable the SIP client of the CM (which might be a Thomson modem with built in telephony functionality and RJ11 jacks for PSTN phones). Due to the fact that all of the traffic is in clear, also the SIP registration (includes credentials) can be captured. An attacker might forge his own SIP/VoIP client to make phone calls (using someone else's telephone number) or also route the phone calls via the malicious SIP/VoIP connection.

Shared secret usage An attacker might want to manipulate a configuration file and use his own crafted or altered one. In order to mitigate this vulnerability DOCSIS introduced a shared secret (CMTS MIC). If a shared secret was actually used for configuration, then the file generation can be checked. The received file includes the CMTS MIC at the end of the file (before the EOF file marker `FF` and perhaps padding) and after the CM MIC. A malicious person can now generate a keyed hash (using

MD5 digest) using the received configuration file parameters and compare the result with the captured CMTS MIC. If the result is the same, no adequate secret was being used at the configuration file generation and anybody could generate his own valid CM configurations. The easiest way to do such a check is as follows: the transferred and captured CM configuration can be decoded to a textual representation (including the CMTS MIC as comment) with the program `docsis`, as described in chapter 3. The DOCSIS CM configuration file parameters can be encoded again. The output is the binary DOCSIS CM file and the CMTS MIC printed to the console, which can be compared to the decoded received CMTS MIC. This check was also done at the first received configuration file (`auto/docsis_modem_4097.bin`) and it uses the shared secret `EURO` for configuration files (this is the default for many DOCSIS configuration file editors in Europe). Therefore, the provider is vulnerable to configuration file alteration attacks.

Of course, there is also a probability that the CMTS does not use the CMTS MIC in any case and therefore the DOCSIS security feature is not used by the providers CMTS. In this case the provider network is vulnerable to configuration file attacks and an attacker can easily steal services.

Meta information The providers deploys 8 downstream channels with 256-QAM modulation. In the upstream direction also 8 channels are announced by the CMTS in the UCD messages at this particular node. Each of them is a QPSK modulated 6.4 MHz wide channel and provides 10.24 Mbit/s throughput. Such wide channels got introduced with DOCSIS 2.0, but a compliant DOCSIS 2.0 modem must meet BPI+ requirements. Therefore, it makes no real sense to disable privacy features, except if there are buggy and non compliant modems deployed in the provider's cable network. The throughput of the whole downstream can be up to 400 Mbit/s and in the upstream direction up to 81.92 Mbit/s. At the analysis 4.049.716.953 Bytes were captured in 1826 seconds, which translates to a bandwidth of roughly 17.74 Mbit/s (maximum is 50 Mbit/s, single channels might be over-utilized), so there was no big over-booking at time.

Because of the disabling of security all traffic is in plain-text and, therefore, many more analyses could be done on the DOCSIS payload's data. However, this is not the main topic of this thesis and, therefore no further analysis was performed.

5.3.2.2. Analysis on different Media

The provider also offers FTTH internet, which uses GPON as the signal transfer technology. It is also possible to use the same cable for regular digital and analogous TV by the use of a different signal carrier. The second provider seems to bridge all the TV-channels and also the DOCSIS channels in the headend to the fiber-optics of the FTTH plant. This means each FTTH-subscriber also receives the DOCSIS signals.

Analogous to the normal cable analysis are the same frequencies used for the DOCSIS downstream channels. Nevertheless, the channel IDs are different (9 to 16). It is very likely that the provider tries to offer DOCSIS over FTTH/PON. This is possible, as there is also a signal carrier on the fiber for upstream signals dedicated to enable the full-duplex transmission mode to employ DOCSIS. It is also very likely that the provider does not use the same physical DOCSIS channels for both networks (cable and PON), because of the different received channel IDs. The security, network and meta information are analogous to the one found in the analysis before, no data encryption (no BPI+, no EAE) is used. All data is transmitted in plain-text. The IPs and MAC addresses are also the same, which translates to the conclusion that the same CMTS is connected to the fiber (PON) and coax (or HFC) cable plant. Moreover, the upstream parameters in the UCD messages are also the same (6.4 MHz QPSK channels).

5.3.3. International Providers

In [96] there is a `pyhton` tool mentioned for sniffing BPKM messages which reports if DES or AES is used and the key length. Moreover, it also checks if the MDD messages contain the EAE feature; it also needs a DVB or ATSC card to do the capturing. Furthermore, there are big American cable providers mentioned with their security parameters. One of the biggest internet access companies named *Comcast* has EAE disabled and for data encryption the DES cipher is used. These insecure settings are also found for *Time Warner* company. [96]

5.3.4. Provisioning Systems

Another source of interesting DOCSIS parameters at provider networks are provisioning systems. During the case study some commercially available DOCSIS provisioning systems were detected too, and one of them reveals CMTS configuration files to the public. The provisioning system should never give insights into the architecture because of the huge attack vector of DOCSIS systems due to their use of many services. Of course, also security by obscurity is no good idea, but the ways a CMTS DOCSIS security part is configured can already reveal a lot to malicious persons. One of the public CMTS configurations [8] is now further analyzed.

```
1 cable modem max-cpe 16
2 cable qos permission modems
3 cable load-balance exclude modem 00XX.9f7e.e0XX
4 cable load-balance exclude modem 00XX.9f54.c5XX
5 username cto@Y.com privilege 15 password 7 ...
6 username Y privilege 15 password 7 ...
7 ip ftp username config@Y.net
```

[8] `https://www.redzaclechner.at/config/uBR7246vxr/dablander/startup-config`

```
8  ip ftp password 7 02231D6628340106587C1C0FXX
9  interface GigabitEthernet0/2
10  ip address X.128.108.10 255.255.255.252
11 interface GigabitEthernet0/3
12  ip address 10.10.180.10 255.255.255.128
13 interface Cable3/0
14  cable bundle 1
15 interface Bundle1
16  description Docsis
17  ip address 172.16.0.1 255.255.252.0 secondary
18  ip address X.128.110.254 255.255.255.0
19  cable arp filter request-send 3 2
20  cable arp filter reply-accept 3 2
21  cable source-verify dhcp
22  cable dhcp-giaddr primary
23  cable helper-address 10.10.180.11
24  no keepalive
25 snmp-server community YRC2012 RO 10
26 snmp-server community public RO 10
```

Listing 5.4: Public CMTS config file excerpt

Listing 5.4 shows the major DOCSIS security relevant parts. It is the same CMTS as used in the scenario attacks, because the device is stated in the configuration file (full file can be found in the appendix). First of all the basic parameters are also in the original configuration, e.g., some downstream and upstream channels are configured for certain frequencies and their affiliation is also stated in the description of the interfaces. The first observation is the lack of any DOCSIS privacy commands. Therefore, no encryption or BPI level (e.g., BPI+ with certificates) is enforced. It is obvious that nearly all downgrade attacks will very probably work. It only depends on the CM configuration file and the CMs features which security measurements will be enabled, but if a malicious person can enforce the usage of other configurations he could also change those parameters. The next observation is the limitation of the CM CPE attached equipment count. This is a good option, as an attacker might change the DOCSIS config file to some very high CPE limit, thus overloading the available MAC space for internet devices (e.g., usually PCs or routers connected to CMs). However, the limit is also a little bit high (16) and therefore an attacker could allocate 16 CPE MAC addresses and perhaps many more IP addresses to each of those MAC addresses. Cable providers usually sell their internet subscriptions based on the given bandwidth. An attacker could easily alter the settings through a malicious CM, because modems have the permission to create quality of service (including speed) settings. DOCSIS networks are vulnerable to ARP broadcast attacks, which may overload the whole network (ARP storm), thus creating a denial of service attack. However„ it is very easy to start such an attack by connecting two CMs to the same segment with their CPE interfaces, because there is no STP enabled. The provider specified a limit for ARP packets on a per SID

basis in a given time period and thus limits the success of such DoS attacks (lines 19-20). Moreover, the provider uses SAV (source address verification) to verify the origin of data packets (e.g., only valid CPE devices behind the proper CM can send and receive data). The next interesting feature is the activation of a SNMP agent on the device. Of course, SNMP offers a lot of functionality to a device (e.g., configure parameters remotely). In this case only read access is possible. This also provides interesting information to an attacker (e.g., MAC addresses of CMs), which enable other attacks (imitating someone's CM). Moreover, the configuration already includes some CM MAC addresses, because they are stated in the load.-balancing exclude group. An attacker might use them to imitate the subscription or also for other attacks (e.g., DoS through high bandwidth usage). Beside the DOCSIS relevant settings, also username with the encrypted password for accessing the device can be found inside the configuration. Moreover, an ftp username and (also encrypted) password is stated.

5.4. Conclusion

The case study of the providers was done completely passive. This means there exist nearly no chance of detection by the provider. Even a short capture of found DOCSIS channels (which is very easy) can lead to tons of information, even if the payload is encrypted. An attacker may perform active attacks and with the ability to send data to the system much more analysis can be done and vulnerability findings are very likely. Impersonation of modems without BPI+ is very likely possible. The MAC addresses found can already reveal interesting information about the system: vendor, perhaps also the production year (big vendors usually have many MAC ranges and may consecutively fill them up). Even if the first tested provider principally uses DOCSIS privacy features, they are not fully established in the whole cable network. Apart from that there are no signs by any cable operator of intending to use and support the better cipher algorithm AES. The reasons may be old hardware or firmware bugs; as a consequence, many of the attacks mentioned in previous chapters are very likely to be executed successfully.

Of course, there can be many more evaluations done on the traffic. Especially relationships and high bandwidth/packet users can be identified (who may have a virus or other high resource consuming things). Another possibility is to examine a relationship between those interesting MAC addresses, the time and date and the pre-equalization value in order to identify the rough location in the cable network.

The found issues and interesting informations were reported to the providers. Provider II replied with a hint of outsourcing the DOCSIS management using a company which specializes in the DOCSIS administration field, but no real signs of a change were given. Provider I doesn't reply until the finalization of this thesis with a real technical answer. Most of the international providers (especially in the US region) claim to comply with national regulatories and take customer satisfaction seriously. Unfortunately regulators

only mention encryption of the traffic needs to be done to keep data privacy (regardless of the cipher, so DES 40 bit is treated as reasonable).

Chapter 6.

Future work and outlook

This chapter describes additional opportunities regarding the security, management, authentication and authorization features of DOCSIS. Many theoretical aspects can be further evaluated, like the provisioning process or the security implementation of data encryption. Moreover, some of those considerations can be used for other carrier technologies, like PON, to render them more secure as well. Practical implementations can help to explore the functionality and the applicability in real environments. Furthermore, it is possible to develop systems to help cable engineers to detect problems regarding the security of their cable networks or to spot attacks and physical issues before customers get dissatisfying experiences.

6.1. Theoretical study

Like the previous chapter has shown, big security vulnerabilities may easyily result from a basic DOCSIS architecture. There are plenty of possibilities to decrease the problems of the issues found. The considerations can go so far as to question if DOCSIS is really a good protocol and standard for cable networks, or if a new architecture should be more target-aimed.

Management of cable networks As cable networks are very big and have a huge number of subscriber devices, their management is very important. The efficient and secure offering of highly available services is evident to meet customer expectations. In order to offer many additional services SNMP is used in DOCSIS, e.g., to set the WiFi password of the router, included into the residential gateway (which also contains the CM part). Automation of tasks (e.g., setting new parameters for a group of cable modems) and consolidation of faults should be considered to keep manual work for a provider at its minimum (e.g., if many cable modems fail, lots of problems would be detected in the headend's management station, but this is usually not the real problem). Such thoughts are developed in [43], but might be taken further.

DOCSIS security at lower layers Further analysis of MAC layer attacks and spoofing may lead to new insights. Moreover, injection attacks in the upstream and also in the downstream can reveal additional issues. A solution to counter simple upstream signal injection might be to develop a DOCSIS RF signal switch. Depending on properties (e.g., power level, SID, or MAP received from additional DS port) of received signals only the right CMs can send signals to the headend, which makes the upstream path more secure and less error noise will occur, leading to a higher CM to CMTS upstream port ratio.

PON In their structure, passive optical networks are like cable networks (coax/HFC). Analogous to this paper, studying security problems of PONs may also lead to similar results. Therefore, many of the ideas, attacks and countermeasures of this thesis may be applied to PON systems. A test system using an ONU and an OLT (and splitters) might be built to check for security issues and especially how the provisioning works in such networks. The provisioning is also often a problem because the specifications do not encounter considerations for a real provider network. Therefore it is very interesting how such a vendor solution can be used (using the built PON system) to service customer devices (including in respect to their subscription, e.g. bandwidth limitations and QoS settings). Another interesting aspect similar to this thesis is sniffing ability. Due to the use of an optical media the eavesdropper needs different hardware. One solutions might be to use a media adapter or a modified optical network termination device (modem).

Legacy systems Many of the security vulnerabilities of DOCSIS found (e.g. downgrade attacks) are the result of compatibility features. How to operate old hardware in new systems securely, without having pitfalls for new standards (e.g., DOCSIS 3.1 and 1.0 compatibility) may be another topic of investigation. One solution might be to operate a legacy system on the same physical structure (besides the new DOCSIS network), but with additional monitoring and detection systems. A IDS/IPS could be developed or an existing one (e.g. `Snort`) might be upgraded to support the detection of malicious DOCSIS modems (e.g. by checking their provisioning procedure, are all parameters in adequate levels, proper timings, are hardware dependent signal parameters not changed rapidly, etc.).

Decryption attacks Active attacks regarding the applied cryptography mechanisms applied in DOCSIS communication may lead to the detection of new vulnerabilities and might show ways of fixing them. Oracle attacks have a huge potential to offer indications for malicious people. Such ideas are also presented in [97], and further analysis of such types of attack may also automate many attacks (e.g., revealing the private key of the CM, rather than finding implementation issues to have access to the CM's memory).

Scyther-proof of BPI/SEC Analyzing the security protocols of DOCSIS with the tool or mechanism `scyther` (tool for automatic verification of security protocols) may lead to new vulnerabilities. Modeling the BPKM and other protocols used in BPI+ and SEC specifications can be very interesting. This drawings can further by proofed with `scyther-proof` to do a proper security proof.

6.2. Practical ideas

This section shortly describes ideas for practical implementations of architectures, programs and systems to make DOCSIS networks more secure.

eDOCSIS and VPN features More and more residential and advanced DOCSIS gateways were developed by various vendors. They offer many more features in addition to those of traditional bridge cable modems. Moreover, upper layer applications and protocols may be used to make the data communication in cable networks more secure. `MACsec`, VPNs (`IPSec`, `OpenVPN`) might be embedded into the DOCSIS cable modem to form a secure channel of transmission. Of course, more features often correspond to a higher attack vector, therefore those features must be checked regarding their architectural design and the practical implementations.

Provisioning system Most of the attacks concerning the headend provisioning system, which usually maps subscribers to devices at the cable modem termination systems [30]. The overall provisioning process must be considered. DOCSIS states only the needed services but does not state its secure application to make the provisioning process as secure as possible. A provisioning system could be designed, which only allows traffic to flow at the right provisioning step and checks if the received and sent data is credible (e.g., by checking if the CM is really registering in the right stage at the legitimate CMTS and its port). Of course, it would be interesting to develop your own secure provisioning system and further analyze vulnerabilities, so that cable providers could benefit from those considerations. Moreover, such a new system might be equipped with an optimized IDS and IPS to prevent additional attacks and vulnerabilities. Additionally regular checks and verification should be done to automatically find potential issues.

Software modules for security statistics As seen in the case study, many issues and vulnerabilities can be found by passively sniffing a DOCSIS network. Integrating and automating the revealing of potential issues can be of high interest. Software modules for `pom-ng` or for distinct cable modems might be developed. Most of the actions done in the case study can be automated, and a `pom-ng` input module (e.g.,

`docsis_security_scan` might be implemented which does the scanning of frequencies, the tuning to it, the capturing and analyzing the DOCSIS packets (e.g., if BPI/EAE is enabled, which cipher do CMs choose, etc.). Cable providers may use such systems to automatically and periodically test their systems, especially if changes were made. If security holes are found, the system could also interact with an IDS or IPS to prevent attacks or the system might be embedded in an already existing IDS/IPS.

Open source modems A big topic is security vulnerabilities and implementation issues of cable modems. Like Kerckhoffs' principle to improve the quality of cryptography has shown, a similar principle might also increase the implementation quality of the firmware for cable modems. It would be advantageous if there was a reference implementation for CMs, similar to the Linux kernel for all of its distributions. Of course, that principle can be applied to any of the needed software. Moreover, this approach should also be used when developing hardware for a cable modem or for any device contained in a DOCSIS environment.

DOCSIS fuzzer CableLabs offers a certification process which tests some basic features to comply with the specification. This inspection is insufficient, as there might exist other bugs in the CMTS or the CM. Therefore, fuzzers could be applied or developed to a DOCSIS environment for testing each component for the correct behavior (e.g. determining if the CMTS respond correctly to a CM state or message).

Chapter 7.

Conclusions

DOCSIS is very successful and were developed fast to offer internet and data connectivity for many customers. The cables were out there in the field and their usage eliminated the need for big alterations. Therefore, the cable providers could provide alternatives to other technologies, such as DSL and were in competition with those.

How the DOCSIS standards work and which considerations regarding security were done was discussed first. Due to some vulnerabilities in the first version the main security specification, called BPI, was also enhanced to include authentication using digital certificates. Therefore, cloning attacks are harder to execute successfully.

A practical DOCSIS network, including the headend with its CMTS and provisioning system, a small cable plant including cable modem and splitters were established to execute security-related attacks. This part shows practical security issues, and with each attack, the network got improved to mitigate for the found problems (e.g., cloning). Even passive attacks, which are nearly undetectable, reveal lots of information, such as MAC addresses and traffic flows.

Furthermore, theoretical issues of the security protocols in DOCSIS are evaluated. Physical issues are stated, such as cable modem swaps, which may enable certain attacks to work. Also, upstream sniffing and methods for deciphering the encrypted DOCSIS data may reveal private information. DOCSIS networks are also vulnerable to active attacks, such as DoS, Man-in-the-middle, up to network and insider attacks. Mitigation is not always easy, but considerations to make it at least more difficult are carried out (e.g., proper CMTS and provisioning system settings). Moreover, implementation issues and legal considerations sometimes hinder cable networks to be as secure as possible.

Moreover, a case study of real cable networks was done. The results are problematic. Neither of the two providers applied the most secure features which are included in DOCSIS, and the best encryption algorithm which was used was DES with 56-bit key size. It was sometimes possible to see all traffic in clear and the receipt of DHCP, SNMP messages and CMs configuration files were possible. Those revealed many provisioning parameters (e.g., bandwidth, CM SNMP agent access, privacy settings). This provider

also has the DOCSIS channels on its FTTH network, which makes the situation even worse. It is very insecure to deactivate EAE at a real big cable company because most of the interesting information (e.g., MAC addresses, IPs in DHCP messages and the CMs configuration file) can be sniffed. Malicious persons may have an easy task to impersonate someone else on those networks or to execute other attacks successfully.

Cable providers must learn that the switch from uni-directional TV to a bi-directional data network also embeds a change in the threat model. Only configuring the basic settings for DOCSIS to make things work is not enough if you want to offer a secure internet service to customers.

Appendix A.

Appendix

This chapter lists all major configurations, environment considerations and products to verify results.

A.1. Practical DOCSIS networks

A.1.1. Components

List of components used for the lab cable plant environment:

- RF attenuators: 2x braun teleCom AT-20 (20dB attenuation), 1x braun teleCom AT-10 (10dB attenuation)
- RF diplexer: 1x braun teleCom DPX-1-65 (Attenuation barrier: 55 dB, IN: 5-862 MHz, OUT1: 5-65 MHz, OUT2: 87-862 MHz)
- RF filters: 1x braun teleCom M-HPF-85 (Return channel blocker 5-65 MHz, Allowed frequency: 85-1000 MHz), 1x axing SZU 14-00 FM-FF (DC-Blocker)
- RF splitters: 1x braun teleCom XS 02e (2 times splitter, 3.5dB attenuation)
- RF cables: 5x 1.5m length Hirschmann Koka 2200 (75 Ohm) with F-type sockets on each end

A.1.2. Configuration files

Configuration files for devices:

A.1.2.1. Provisioning system

The provisioning system must offer IP addresses in the appropriate ranges to the CM and CPE devices. Following list is used for the ISC-DHCPD:

```
#lease times
default-lease-time 600;
max-lease-time 7200;

#syslog server
option log-servers 172.16.0.1;

#ToD time server
option time-servers 172.16.0.1;

#TFTP server
#Old (pre DOCSIS 3.0) modems use the next-server field of the DHCP message
next-server 172.16.0.1;

# DOCSIS 3.0+ modems only use next-server if the vivso.2 option is not available
# The newer vivso.2 option allows multiple addresses and thus fallback mechanisms
# Due to some limitations in the ISC dhcpd configuration, we need to encode this in
# hexadecimal, so let's do this:
#option vivso 00:00:11:8b:0a:02:08:0a:10:00:04:0a:11:00:04;

# Subnet configuration
# The DHCP server needs a subnet declaration for at least one of the provisioning interfaces,
# so we assume the provisioning interface (the interface used by the relay-agent of the CMTS
# is 10.16.0.5.  We also don't want this DHCP server to provision our backend, so we declare
# the network, but don't allow the server to hand out any leases
subnet 172.16.0.0 netmask 255.255.255.0 {
    ignore booting;
}

shared-network CMTS1{

#subnet for CMs at the CMTS
subnet 10.0.1.0 netmask 255.255.255.0 {
    range 10.0.1.10 10.0.1.254;
    option broadcast-address 10.0.1.255;
    option routers 10.0.1.1;
    default-lease-time 23200;
    max-lease-time 86400;
```

```
39      #only cable modems with known MAC address get IP addresses
40      deny unknown-clients;
41  }
42
43  #subnet for CPEs
44  subnet 192.168.50.0 netmask 255.255.255.0 {
45      range 192.168.50.10 192.168.50.254;
46      option routers 192.168.50.1;
47      option broadcast-address 192.168.50.255;
48
49      default-lease-time 3600;
50      max-lease-time 7200;
51      #the CPE MACs can be anything, we don't want to manage them
52      allow unknown-clients;
53  }
54
55  #CMs MAC assignments
56  host cm-subscriber1 {
57      hardware ethernet 00:24:d1:d2:77:d7;
58      filename "start2.cm";
59      option bootfile-name "start2.cm";
60  }
61
62  host cm-subscriber2 {
63      hardware ethernet 00:18:c0:1d:90:a2;
64      filename "start1.cm";
65      option bootfile-name "start1.cm";
66  }
67
68  host cm-subscriber3 {
69      hardware ethernet aa:bb:cc:dd:ee:ab;
70      filename "start1.cm";
71      option bootfile-name "start1.cm";
72  }
73
74  host cm-subscriber4 {
75      hardware ethernet 00:11:22:33:44:55;
76      filename "start1.cm";
77      option bootfile-name "start1.cm";
78  }
79
80  }
```

Listing A.1: Initial DHCP server configuration

The following listing is used for the SNMP daemon to receive SNMP traps from CMs (e.g. some Motorola CMs send trap logs)

```
#  Listen for connections from the local system only
agentAddress  udp:127.0.0.1:161
#  Listen for connections on all interfaces (both IPv4 *and* IPv6)
#agentAddress udp:161,udp6:[::1]:161

#  ACCESS CONTROL
                                                #  system + hrSystem groups only
view   systemonly  included   .1.3.6.1.2.1.1
view   systemonly  included   .1.3.6.1.2.1.25.1
 rocommunity public  default    -V systemonly
                                                #  rocommunity6 is for IPv6
 rocommunity6 public  default   -V systemonly

 rouser   authOnlyUser
                                              #  Full write access for encrypted↩
                                                  ↪ requests
sysLocation    Provider headend
sysContact     cablelabs@provider
                                               # Application + End-to-End layers
sysServices    72
```

Listing A.2: SNMPD configuration file (snmpd.conf)

Additionally to the SNMP daemon configuration file an extra configuration is used to configure trap reception:

```

authCommunity log cablelab
## send mail when get any events
#traphandle default /usr/bin/traptoemail -s smtp.example.org foobar@example.org
#
## send mail when get linkDown
#traphandle .1.3.6.1.6.3.1.1.5.3 /usr/bin/traptoemail -s smtp.example.org ↩
    ↪foobar@example.org
```

Listing A.3: SNMPTRAPD configuration file (snmptrapd.conf)

Some CMs use SYSLOG to provide the ability to receive logging and system information from the remote devices. Following list is a sample rsyslog configuration file:

```
$ModLoad imuxsock # provides support for local system logging
$ModLoad imklog   # provides kernel logging support
#$ModLoad immark  # provides --MARK-- message capability

# provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514

```

```
9  # provides TCP syslog reception
10 $ModLoad imtcp
11 $InputTCPServerRun 514
12
13 # Use traditional timestamp format.
14 # To enable high precision timestamps, comment out the following line.
15 $ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat
16
17 # Set the default permissions for all log files.
18 $FileOwner root
19 $FileGroup adm
20 $FileCreateMode 0640
21 $DirCreateMode 0755
22 $Umask 0022
23
24 # Where to place spool and state files
25 $WorkDirectory /var/spool/rsyslog
26
27 # First some standard log files.  Log by facility.
28 auth,authpriv.*         /var/log/auth.log
29 *.*;auth,authpriv.none      -/var/log/syslog
30 daemon.*            -/var/log/daemon.log
31 kern.*              -/var/log/kern.log
32 lpr.*               -/var/log/lpr.log
33 mail.*              -/var/log/mail.log
34 user.*              -/var/log/user.log
35
36 # Logging for the mail system.  Split it up so that
37 # it is easy to write scripts to parse these files.
38 mail.info           -/var/log/mail.info
39 mail.warn           -/var/log/mail.warn
40 mail.err            /var/log/mail.err
41
42 #
43 # Logging for INN news system.
44 #
45 news.crit           /var/log/news/news.crit
46 news.err            /var/log/news/news.err
47 news.notice         -/var/log/news/news.notice
48
49 #
50 # Some "catch-all" log files.
51 #
52 *.=debug;\
53     auth,authpriv.none;\
54     news.none;mail.none -/var/log/debug
55 *.=info;*.=notice;*.=warn;\
```

```
56     auth,authpriv.none;\
57     cron,daemon.none;\
58     mail,news.none      -/var/log/messages
```

Listing A.4: SYSLOG configuration file (rsyslog.conf)

The configuration file for the modems look in text representation like this:

```
1  Main
2  {
3    NetworkAccess 1;            /* enables packet forwarding */
4    GlobalPrivacyEnable 0;      /*  privacy */
5    UsServiceFlow               /* creates an upstream service flow */
6    {
7      MaxRateSustained 100000;  /* limit to 100 kbit/s */
8      UsServiceFlowRef 1;       /* SF number */
9      QosParamSetType 7;        /* activates SF */
10   }
11
12   DsServiceFlow               /* creates an downstream service flow */
13   {
14     MaxRateSustained 1000000; /* limit to 1000 kbit/s */
15     DsServiceFlowRef 2;       /* SF number */
16     QosParamSetType 7;        /* activates SF */
17   }
18   /* Allow SNMP public reads */
19   SnmpMibObject docsDevNmAccessIp.1 IPAddress 0.0.0.0 ;
20   SnmpMibObject docsDevNmAccessIpMask.1 IPAddress 0.0.0.0 ;
21   SnmpMibObject docsDevNmAccessCommunity.1 String "public" ;
22   SnmpMibObject docsDevNmAccessControl.1 Integer 2; /* read */
23   SnmpMibObject docsDevNmAccessStatus.1 Integer 4; /* createAndGo */
24   /* Allow SNMP private writes */
25   SnmpMibObject docsDevNmAccessIp.2 IPAddress 0.0.0.0 ;
26   SnmpMibObject docsDevNmAccessIpMask.2 IPAddress 0.0.0.0 ;
27   SnmpMibObject docsDevNmAccessCommunity.2 String "private" ;
28   SnmpMibObject docsDevNmAccessControl.2 Integer 3; /* readWrite */
29   SnmpMibObject docsDevNmAccessStatus.2 Integer 4; /* createAndGo */
30 }
```

Listing A.5: Cable modem DOCSIS configuration file (start1)

The CM configuration can be encoded using the tool `docsis` to get a readable file for the CMs (which can be loaded by the CMs using TFTP). The configuration includes settings to allow SNMP read and write access (using SNMPv2c) to those CMs which apply this file at registration. First the allowed IP address range (lines 19, 25, value 0.0.0.0) and the mask (lines 20, 26, value 0.0.0.0 for all) are set. Moreover the community strings are set for SNMP reads (line 21: public) and writes (line 27: private). Because

one MIB-object for the private and one for the public SNMP access is created the appropriate access controls must be set (lines 22, 28). The last step is to create those two SNMP settings (lines 23, 29).

Analogously to the above CM configuration file the following file was created for another CM (the difference is the max. allowed bandwidth):

```
1  Main
2  {
3    NetworkAccess 1;            /* enables packet forwarding */
4    GlobalPrivacyEnable 1;      /* privacy */
5    UsServiceFlow               /* creates an upstream service flow */
6    {
7      MaxRateSustained 200000;  /* limit to 200 kbit/s */
8      UsServiceFlowRef 1;       /* SF number */
9      QosParamSetType 7;        /* activates SF */
10   }
11
12   DsServiceFlow               /* creates an downstream service flow */
13   {
14     MaxRateSustained 2000000; /* limit to 2000 kbit/s */
15     DsServiceFlowRef 2;       /* SF number */
16     QosParamSetType 7;        /* activates SF */
17   }
18   /* Allow SNMP public reads */
19   SnmpMibObject docsDevNmAccessIp.1 IPAddress 0.0.0.0 ;
20   SnmpMibObject docsDevNmAccessIpMask.1 IPAddress 0.0.0.0 ;
21   SnmpMibObject docsDevNmAccessCommunity.1 String "public" ;
22   SnmpMibObject docsDevNmAccessControl.1 Integer 2; /* read */
23   SnmpMibObject docsDevNmAccessStatus.1 Integer 4; /* createAndGo */
24   /* Allow SNMP private writes */
25   SnmpMibObject docsDevNmAccessIp.2 IPAddress 0.0.0.0 ;
26   SnmpMibObject docsDevNmAccessIpMask.2 IPAddress 0.0.0.0 ;
27   SnmpMibObject docsDevNmAccessCommunity.2 String "private" ;
28   SnmpMibObject docsDevNmAccessControl.2 Integer 3; /* readWrite */
29   SnmpMibObject docsDevNmAccessStatus.2 Integer 4; /* createAndGo */
30 }
```

Listing A.6: Cable modem DOCSIS configuration file (start2)

During the practical scenarios the CM config was enhanced (allow BPI):

```
1  Main
2  {
3    NetworkAccess 1;            /* enables packet forwarding */
4    GlobalPrivacyEnable 1;      /* enables BPI(encryption) */
5    UsServiceFlow               /* creates an upstream service flow */
6    {
```

```
7     UsServiceFlowRef 1;       /* SF number */
8     QosParamSetType 7;        /* activates SF */
9   }
10
11  DsServiceFlow               /* creates an downstream service flow */
12  {
13    DsServiceFlowRef 2;       /* SF number */
14    QosParamSetType 7;        /* activates SF */
15  }
16
17 }
```

Listing A.7: Cable modem DOCSIS configuration file (scenario BPI)

The following list is the configuration file for the unallowed service usage scenario:

```
1  Main
2  {
3    NetworkAccess 1;            /* enables packet forwarding */
4    GlobalPrivacyEnable 0;      /* don't care about privacy */
5    MaxCPE 254;                 /* allow upto 255 CPE MACs */
6    UsServiceFlow               /* creates an upstream service flow */
7    {
8      UsServiceFlowRef 1;       /* SF number */
9      QosParamSetType 7;        /* activates SF */
10     TrafficPriority 7;        /* set priority to highest */
11   }
12
13   DsServiceFlow               /* creates an downstream service flow */
14   {
15     DsServiceFlowRef 2;       /* SF number */
16     QosParamSetType 7;        /* activates SF */
17     TrafficPriority 7;        /* set priority to highest */
18   }
19 }
```

Listing A.8: Cable modem DOCSIS configuration file (scenario unallowed service)

```
1  Main
2  {
3    NetworkAccess 1;            /* enables packet forwarding */
4    ModemCapabilities
5    {
6      BaselinePrivacySupport 0; /* disable BPI feature at the CM */
7    }
8    UsServiceFlow               /* creates an upstream service flow */
9    {
10     UsServiceFlowRef 1;       /* SF number */
```

```
    QosParamSetType 7;        /* activates SF */
  }

  DsServiceFlow               /* creates an downstream service flow */
  {
    DsServiceFlowRef 2;       /* SF number */
    QosParamSetType 7;        /* activates SF */
  }
}
```

Listing A.9: Cable modem DOCSIS configuration file (scenario downgrade)

A.1.2.2. CMTS

The headend contains the CMTS, which was configured according to the following settings (through serial console and/or telnet and or SSH):

```
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname CMTS1
boot-start-marker
boot system flash disk2:ubr7200-jk9su2-mz.122-33.SCF5.bin
boot system flash disk2:ubr7200-jk9su2-mz.122-33.SCF.bin
boot system flash disk2:ubr7200-ik9su2-mz.123-17a.BC.bin
boot-end-marker
enable secret 5 $1$HlQl$ROO5sJ8kiZLFx0ovzCbnD/
no aaa new-model
no cable admission-control preempt priority-voice
cable freq-range european
no cable qos permission create
no cable qos permission update
cable qos permission modems
cable logging badipsource #log all detected issues
cable logging layer2events #log all detected issues
cable logging overlapip #log all detected issues
ip subnet-zero
no ip domain lookup
ip domain name cablelab
ip cef
multilink bundle-name authenticated
call rsvp-sync
username cisco password 7 14141B180F0B
interface GigabitEthernet0/1
 description to Provisioning server (172.16.0.1)
```

```
 ip address 172.16.0.3 255.255.255.0
 media-type rj45
 speed auto
 duplex auto
 negotiation auto
interface GigabitEthernet0/2
 description Uplink (GW 192.168.100.254)
 ip address 192.168.100.3 255.255.255.0
 media-type rj45
 speed auto
 duplex auto
 negotiation auto
interface Cable3/0
 no cable packet-cache
 cable bundle 1
 cable downstream channel-id 1
 cable downstream annex A
 cable downstream modulation 256qam
 cable downstream frequency 443000000
 no cable downstream rf-shutdown
 cable upstream max-ports 4
 cable upstream 0 connector 0
 cable upstream 0 frequency 27000000
 cable upstream 0 channel-width 1600000 1600000
 cable upstream 0 docsis-mode tdma
 cable upstream 0 minislot-size 4
 cable upstream 0 range-backoff 3 6
 cable upstream 0 modulation-profile 41
 no cable upstream 0 shutdown
interface Bundle1
 ip address 192.168.50.1 255.255.255.0 secondary
 ip address 10.0.1.1 255.255.255.0
 no cable arp filter request-send
 no cable arp filter reply-accept
 cable helper-address 172.16.0.1
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.100.254
no ip http server
no ip http secure-server
ip http client username cisco
logging cmts ipc-cable log-level debugging #log everything
cpd cr-id 1
nls resp-timeout 1
no cdp run
control-plane
dial-peer cor custom
gatekeeper
```

```
 shutdown
line con 0
 password 7 045802150C2E
 login
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 password 7 01100F175804
 login local
 transport input ssh
line vty 5 15
 login
exception crashinfo buffersize 64
end
```

Listing A.10: CMTS Initial configuration

A.2. Case Study

The case study involved some hardware and software components, which are stated here.

A.2.1. Components

PC-Hardware for eavesdropping is the following (Standard-PC):

- Model: Asus U30SD
- CPU: Intel Core i5-2410
- RAM: 4 GB DDR3
- HDD: Intenso SSD 128GB
- USB 2.0 port for the DVB-C receiver stick

A.2.1.1. Software

To talk to the signal receiver device a driver is needed. Due to some issues the driver was altered:

RTL2832P/MN88473 demodulator driver The patch for mitigating I2C errors due to RC polling is very simple:

```
[line 1190] -   rc->interval = 400;
[line 1190] +   rc->interval = 200;
[line 1292] -   rc->interval = 400;
[line 1292] +   rc->interval = 200;
```

Listing A.11: I2C polling fix for rtl2832p/mn88473 driver (drivers/media/usb/dvb-usb-v2/rtl28xxu.c)

The already patched version can be downloaded and built this way:

```
git clone git://linuxtv.org/media_build.git
cd media_build
make download
make untar
make stagingconfig
make
./build --git git://linuxtv.org/anttip/media_tree.git astrometa
```

Listing A.12: Building RTL2832P/MN88473 demodulator driver

Installing `pom-ng` (Details for the installation can be found in [65]):

```
git clone git://github.com/gmsoft-tuxicoman/pom-ng.git
autoreconf -f -i
./configure
make
make install
```

Listing A.13: Installing pom-ng

A.2.2. Analysis

During the practical evaluation of real cable provider networks some configuration files and other interesting information was obtained, which is (anonymized) listed here. Some public IP addresses are replaced with `X` to keep the privacy of the providers and the components.

A.2.2.1. Provider II

Received and decoded configuration files The following listings represent the decoded configuration files, which were received during the capture at the case study.

```
1  Network Access Control:on
2  SNMP MIB Object(docsDevNmAccessIp.1):1.3.6.1.2.1.69.1.2.1.2.1, IP Address, X↩
       ↪.255.144.0
3  SNMP MIB Object(docsDevNmAccessIpMask.1):1.3.6.1.2.1.69.1.2.1.3.1, IP Address, ↩
       ↪255.255.255.128
4  SNMP MIB Object(docsDevNmAccessCommunity.1):1.3.6.1.2.1.69.1.2.1.4.1, Octet ↩
       ↪String, public
5  SNMP MIB Object(docsDevNmAccessControl.1):1.3.6.1.2.1.69.1.2.1.5.1, Integer, 3
6  SNMP MIB Object(docsDevNmAccessStatus.1):1.3.6.1.2.1.69.1.2.1.7.1, Integer, 4
7  SNMP MIB Object(unknown OID 1.3.6.1.4.1.1166.1.200.2.35.0)↩
       ↪:1.3.6.1.4.1.1166.1.200.2.35.0, Octet String, 0xE0
8  SNMP MIB Object(unknown OID 1.3.6.1.4.1.1166.1.200.2.36.0)↩
       ↪:1.3.6.1.4.1.1166.1.200.2.36.0, Octet String, 0xE0
9  SNMP MIB Object(unknown OID 1.3.6.1.4.1.2863.205.10.1.33.3.1.8.0)↩
       ↪:1.3.6.1.4.1.2863.205.10.1.33.3.1.8.0, Integer, 2
10 Maximum Number of CPEs:2
11 Upstream Packet Classification Encoding
12   Classifier Reference:1
13   Service Flow Reference:2
14   Rule Priority:50
15   Classifier Activation State:on
16   IP Packet Classification Encodings
17     IP Protocol:256
18     IP Source Address:10.0.0.0
19     IP Source Mask:255.255.0.0
20 Upstream Packet Classification Encoding
21   Classifier Reference:2
22   Service Flow Reference:2
23   Rule Priority:50
24   Classifier Activation State:on
25   IP Packet Classification Encodings
26     IP Protocol:256
27     IP Source Address:X.13.26.0
28     IP Source Mask:255.255.255.128
29 Upstream Packet Classification Encoding
30   Classifier Reference:3
31   Service Flow Reference:2
32   Rule Priority:50
33   Classifier Activation State:on
34   IP Packet Classification Encodings
35     IP Protocol:256
36     IP Source Address:X.13.33.0
37     IP Source Mask:255.255.255.128
38 Downstream Packet Classification Encoding
39   Classifier Reference:11
40   Service Flow Reference:12
41   Rule Priority:50
```

```
  Classifier Activation State:on
  IP Packet Classification Encodings
    IP Protocol:256
    IP Destination Address:10.0.0.0
    IP Destination Mask:255.255.0.0
Downstream Packet Classification Encoding
  Classifier Reference:12
  Service Flow Reference:12
  Rule Priority:50
  Classifier Activation State:on
  IP Packet Classification Encodings
    IP Protocol:256
    IP Destination Address:X.13.26.0
    IP Destination Mask:255.255.255.128
Downstream Packet Classification Encoding
  Classifier Reference:13
  Service Flow Reference:12
  Rule Priority:50
  Classifier Activation State:on
  IP Packet Classification Encodings
    IP Protocol:256
    IP Destination Address:X.13.33.0
    IP Destination Mask:255.255.255.128
Upstream Service Flow Encodings
  Service Flow Reference:1
  Service Class Name:ucountme
  Quality of Service Parameter Set:provisioned admitted active
  Traffic Priority:3
  Upstream Maximum Sustained Traffic Rate:1000000
Upstream Service Flow Encodings
  Service Flow Reference:2
  Quality of Service Parameter Set:provisioned admitted active
  Traffic Priority:5
  Upstream Maximum Sustained Traffic Rate:1024000
Downstream Service Flow Encodings
  Service Flow Reference:11
  Service Class Name:dcountme
  Quality of Service Parameter Set:provisioned admitted active
  Traffic Priority:3
  Downstream Maximum Sustained Traffic Rate:15500000
Downstream Service Flow Encodings
  Service Flow Reference:12
  Quality of Service Parameter Set:provisioned admitted active
  Traffic Priority:5
  Downstream Maximum Sustained Traffic Rate:1024000
Privacy Enable:off
Manufacturer Code Verification Certificate:308...
```

```
89 Manufacturer Code Verification Certificate:4F4...
90 Manufacturer Code Verification Certificate:E41...
91 Manufacturer Code Verification Certificate:131...
```

Listing A.14: Full received CM configuration file

```
1  Downstream Frequency Configuration:506000000
2  Network Access Control:on
3  SNMP MIB Object(docsDevNmAccessIp.1):1.3.6.1.2.1.69.1.2.1.2.1, IP Address, X↩
       ↪.255.144.0
4  SNMP MIB Object(docsDevNmAccessIpMask.1):1.3.6.1.2.1.69.1.2.1.3.1, IP Address, ↩
       ↪255.255.255.128
5  SNMP MIB Object(docsDevNmAccessCommunity.1):1.3.6.1.2.1.69.1.2.1.4.1, Octet ↩
       ↪String, public
6  SNMP MIB Object(docsDevNmAccessControl.1):1.3.6.1.2.1.69.1.2.1.5.1, Integer, 3
7  SNMP MIB Object(docsDevNmAccessStatus.1):1.3.6.1.2.1.69.1.2.1.7.1, Integer, 4
8  SNMP MIB Object(unknown OID 1.3.6.1.4.1.1166.1.200.2.35.0)↩
       ↪:1.3.6.1.4.1.1166.1.200.2.35.0, Octet String, 0xE0
9  SNMP MIB Object(unknown OID 1.3.6.1.4.1.1166.1.200.2.36.0)↩
       ↪:1.3.6.1.4.1.1166.1.200.2.36.0, Octet String, 0xE0
10 SNMP MIB Object(unknown OID 1.3.6.1.4.1.2863.205.10.1.10.1.0)↩
       ↪:1.3.6.1.4.1.2863.205.10.1.10.1.0, Integer, 1
11 SNMP MIB Object(unknown OID 1.3.6.1.4.1.2863.205.10.1.10.2.0)↩
       ↪:1.3.6.1.4.1.2863.205.10.1.10.2.0, Integer, 1
12 SNMP MIB Object(unknown OID 1.3.6.1.4.1.2863.205.10.1.10.3.0)↩
       ↪:1.3.6.1.4.1.2863.205.10.1.10.3.0, Octet String, ...
13 SNMP MIB Object(unknown OID 1.3.6.1.4.1.2863.205.10.1.10.4.0)↩
       ↪:1.3.6.1.4.1.2863.205.10.1.10.4.0, Integer, 1
14 SNMP MIB Object(unknown OID 1.3.6.1.4.1.2863.205.10.1.10.8.0)↩
       ↪:1.3.6.1.4.1.2863.205.10.1.10.8.0, IP Address, X.255.151.8
15 SNMP MIB Object(unknown OID 1.3.6.1.4.1.2863.205.10.1.10.9.0)↩
       ↪:1.3.6.1.4.1.2863.205.10.1.10.9.0, IP Address, 255.255.255.248
16 SNMP MIB Object(unknown OID 1.3.6.1.4.1.2863.205.10.1.10.10.0)↩
       ↪:1.3.6.1.4.1.2863.205.10.1.10.10.0, IP Address, X.255.151.9
17 SNMP MIB Object(unknown OID 1.3.6.1.4.1.2863.205.10.1.10.11.0)↩
       ↪:1.3.6.1.4.1.2863.205.10.1.10.11.0, Integer, 2
18 SNMP MIB Object(unknown OID 1.3.6.1.4.1.2863.205.10.1.10.12.0)↩
       ↪:1.3.6.1.4.1.2863.205.10.1.10.12.0, Integer, 2
19 SNMP MIB Object(unknown OID 1.3.6.1.4.1.2863.205.10.1.10.99.0)↩
       ↪:1.3.6.1.4.1.2863.205.10.1.10.99.0, Integer, 1
20 Maximum Number of CPEs:2
21 Upstream Packet Classification Encoding
22   Classifier Reference:1
23   Service Flow Reference:2
24   Rule Priority:50
25   Classifier Activation State:on
26   IP Packet Classification Encodings
27     IP Protocol:256
```

```
    IP Source Address:10.1.1.0
    IP Source Mask:255.255.0.0
Upstream Packet Classification Encoding
  Classifier Reference:2
  Service Flow Reference:2
  Rule Priority:50
  Classifier Activation State:on
  IP Packet Classification Encodings
    IP Protocol:256
    IP Source Address:X.13.26.0
    IP Source Mask:255.255.255.128
Upstream Packet Classification Encoding
  Classifier Reference:3
  Service Flow Reference:2
  Rule Priority:50
  Classifier Activation State:on
  IP Packet Classification Encodings
    IP Protocol:256
    IP Source Address:X.13.33.0
    IP Source Mask:255.255.255.128
Upstream Packet Classification Encoding
  Classifier Reference:4
  Service Flow Reference:2
  Rule Priority:50
  Classifier Activation State:on
  IP Packet Classification Encodings
    IP Protocol:256
    IP Source Address:X.93.81.128
    IP Source Mask:255.255.255.128
Downstream Packet Classification Encoding
  Classifier Reference:11
  Service Flow Reference:12
  Rule Priority:50
  Classifier Activation State:on
  IP Packet Classification Encodings
    IP Protocol:256
    IP Destination Address:10.1.1.0
    IP Destination Mask:255.255.0.0
Downstream Packet Classification Encoding
  Classifier Reference:12
  Service Flow Reference:12
  Rule Priority:50
  Classifier Activation State:on
  IP Packet Classification Encodings
    IP Protocol:256
    IP Destination Address:X.13.26.0
    IP Destination Mask:255.255.255.128
```

```
75 Downstream Packet Classification Encoding
76   Classifier Reference:13
77   Service Flow Reference:12
78   Rule Priority:50
79   Classifier Activation State:on
80   IP Packet Classification Encodings
81     IP Protocol:256
82     IP Destination Address:X.13.33.0
83     IP Destination Mask:255.255.255.128
84 Downstream Packet Classification Encoding
85   Classifier Reference:14
86   Service Flow Reference:12
87   Rule Priority:50
88   Classifier Activation State:on
89   IP Packet Classification Encodings
90     IP Protocol:256
91     IP Destination Address:X.93.81.128
92     IP Destination Mask:255.255.255.128
93 Upstream Service Flow X%
94   Service Flow Reference:1
95   Service Class Name:ucountme
96   Quality of Service Parameter Set:provisioned admitted active
97   Traffic Priority:3
98   Upstream Maximum Sustained Traffic Rate:4096000
99 Upstream Service Flow Encodings
100  Service Flow Reference:2
101  Quality of Service Parameter Set:provisioned admitted active
102  Traffic Priority:5
103  Upstream Maximum Sustained Traffic Rate:1024000
104 Downstream Service Flow Encodings
105  Service Flow Reference:11
106  Service Class Name:dcountme
107  Quality of Service Parameter Set:provisioned admitted active
108  Traffic Priority:3
109  Downstream Maximum Sustained Traffic Rate:28000000
110 Downstream Service Flow Encodings
111  Service Flow Reference:12
112  Quality of Service Parameter Set:provisioned admitted active
113  Traffic Priority:5
114  Downstream Maximum Sustained Traffic Rate:1024000
115 Privacy Enable:off
116 Manufacturer Code Verification Certificate:308...
117 Manufacturer Code Verification Certificate:031...
118 Manufacturer Code Verification Certificate:D4F...
```

Listing A.15: Full received CM configuration file (second file)

```
1 Network Access Control:on
```

```
SNMP MIB Object(docsDevNmAccessIp.1):1.3.6.1.2.1.69.1.2.1.2.1, IP Address, X.255.144.0
SNMP MIB Object(docsDevNmAccessIpMask.1):1.3.6.1.2.1.69.1.2.1.3.1, IP Address, 255.255.255.128
SNMP MIB Object(docsDevNmAccessCommunity.1):1.3.6.1.2.1.69.1.2.1.4.1, Octet String, ...
SNMP MIB Object(docsDevNmAccessControl.1):1.3.6.1.2.1.69.1.2.1.5.1, Integer, 3
SNMP MIB Object(docsDevNmAccessStatus.1):1.3.6.1.2.1.69.1.2.1.7.1, Integer, 4
SNMP MIB Object(unknown OID 1.3.6.1.4.1.1166.1.200.2.35.0):1.3.6.1.4.1.1166.1.200.2.35.0, Octet String, 0xE0
SNMP MIB Object(unknown OID 1.3.6.1.4.1.1166.1.200.2.36.0):1.3.6.1.4.1.1166.1.200.2.36.0, Octet String, 0xE0
SNMP MIB Object(unknown OID 1.3.6.1.4.1.4413.2.2.2.1.18.1.1.2.1.12.32):1.3.6.1.4.1.4413.2.2.2.1.18.1.1.2.1.12.32, Integer, 2
SNMP MIB Object(unknown OID 1.3.6.1.4.1.4413.2.2.2.1.18.1.1.1.0):1.3.6.1.4.1.4413.2.2.2.1.18.1.1.1.0, Integer, 1
Maximum Number of CPEs:5
Upstream Packet Classification Encoding
  Classifier Reference:1
  Service Flow Reference:2
  Rule Priority:100
  Classifier Activation State:on
  IP Packet Classification Encodings
    IP Protocol:256
    IP Source Address:X.13.40.0
    IP Source Mask:255.255.255.128
Upstream Packet Classification Encoding
  Classifier Reference:2
  Service Flow Reference:3
  Rule Priority:50
  Classifier Activation State:on
  IP Packet Classification Encodings
    IP Protocol:256
    IP Destination Address:X.218.227.2
    IP Destination Mask:255.255.255.255
Upstream Packet Classification Encoding
  Classifier Reference:3
  Service Flow Reference:3
  Rule Priority:50
  Classifier Activation State:on
  IP Packet Classification Encodings
    IP Protocol:256
    IP Destination Address:192.168.0.0
    IP Destination Mask:255.255.0.0
Upstream Packet Classification Encoding
  Classifier Reference:4
  Service Flow Reference:3
```

```
42    Rule Priority:50
43    Classifier Activation State:on
44    IP Packet Classification Encodings
45      IP Protocol:256
46      IP Destination Address:X.192.20.20
47      IP Destination Mask:255.255.255.255
48  Upstream Packet Classification Encoding
49    Classifier Reference:5
50    Service Flow Reference:3
51    Rule Priority:50
52    Classifier Activation State:on
53    IP Packet Classification Encodings
54      IP Protocol:256
55      IP Destination Address:X.13.41.0
56      IP Destination Mask:255.255.255.0
57  Upstream Packet Classification Encoding
58    Classifier Reference:6
59    Service Flow Reference:3
60    Rule Priority:50
61    Classifier Activation State:on
62    IP Packet Classification Encodings
63      IP Protocol:256
64      IP Destination Address:X.218.227.3
65      IP Destination Mask:255.255.255.255
66  Upstream Packet Classification Encoding
67    Classifier Reference:7
68    Service Flow Reference:2
69    Rule Priority:100
70    Classifier Activation State:on
71    IP Packet Classification Encodings
72      IP Protocol:256
73      IP Source Address:X.192.30.128
74      IP Source Mask:255.255.255.128
75  Downstream Packet Classification Encoding
76    Classifier Reference:11
77    Service Flow Reference:12
78    Rule Priority:100
79    Classifier Activation State:on
80    IP Packet Classification Encodings
81      IP Protocol:256
82      IP Destination Address:X.13.40.0
83      IP Destination Mask:255.255.255.128
84  Downstream Packet Classification Encoding
85    Classifier Reference:12
86    Service Flow Reference:13
87    Rule Priority:50
88    Classifier Activation State:on
```

```
  IP Packet Classification Encodings
    IP Protocol:256
    IP Source Address:X.218.227.2
    IP Source Mask:255.255.255.255
Downstream Packet Classification Encoding
  Classifier Reference:13
  Service Flow Reference:13
  Rule Priority:50
  Classifier Activation State:on
  IP Packet Classification Encodings
    IP Protocol:256
    IP Source Address:192.168.0.0
    IP Source Mask:255.255.0.0
Downstream Packet Classification Encoding
  Classifier Reference:14
  Service Flow Reference:13
  Rule Priority:50
  Classifier Activation State:on
  IP Packet Classification Encodings
    IP Protocol:256
    IP Source Address:X.192.20.20
    IP Source Mask:255.255.255.255
Downstream Packet Classification Encoding
  Classifier Reference:15
  Service Flow Reference:13
  Rule Priority:50
  Classifier Activation State:on
  IP Packet Classification Encodings
    IP Protocol:256
    IP Source Address:X.13.41.0
    IP Source Mask:255.255.255.0
Downstream Packet Classification Encoding
  Classifier Reference:16
  Service Flow Reference:13
  Rule Priority:50
  Classifier Activation State:on
  IP Packet Classification Encodings
    IP Protocol:256
    IP Source Address:X.218.227.3
    IP Source Mask:255.255.255.255
Downstream Packet Classification Encoding
  Classifier Reference:17
  Service Flow Reference:12
  Rule Priority:100
  Classifier Activation State:on
  IP Packet Classification Encodings
    IP Protocol:256
```

```
136     IP Destination Address:X.192.30.128
137     IP Destination Mask:255.255.255.128
138 Upstream Service Flow Encodings
139   Service Flow Reference:1
140   Service Class Name:ucountme
141   Quality of Service Parameter Set:provisioned admitted active
142   Traffic Priority:3
143   Upstream Maximum Sustained Traffic Rate:1024000
144 Upstream Service Flow Encodings
145   Service Flow Reference:2
146   Quality of Service Parameter Set:provisioned admitted active
147   Traffic Priority:7
148   Upstream Maximum Sustained Traffic Rate:1024000
149 Upstream Service Flow Encodings
150   Service Flow Reference:3
151   Quality of Service Parameter Set:provisioned admitted active
152   Traffic Priority:6
153   Upstream Maximum Sustained Traffic Rate:1024000
154 Downstream Service Flow Encodings
155   Service Flow Reference:11
156   Service Class Name:dcountme
157   Quality of Service Parameter Set:provisioned admitted active
158   Traffic Priority:3
159   Downstream Maximum Sustained Traffic Rate:17600000
160 Downstream Service Flow Encodings
161   Service Flow Reference:12
162   Quality of Service Parameter Set:provisioned admitted active
163   Traffic Priority:7
164   Downstream Maximum Sustained Traffic Rate:1024000
165 Downstream Service Flow Encodings
166   Service Flow Reference:13
167   Quality of Service Parameter Set:provisioned admitted active
168   Traffic Priority:6
169   Downstream Maximum Sustained Traffic Rate:1024000
170 Privacy Enable:off
171 Euro-DOCSIS vendor specific Extension Field:001095/190...
```

Listing A.16: Full received CM configuration file (third file)

List of abbreviations

ACL Access control list
ADC Analog digital converter
AES Advanced encryption standard
ARP Address resolution protocol
ATSC Advanced Television Systems Committee
BER Bit error rate
BPI Baseline privacy interface
BPKM Baseline privacy key management
CATV Community antenna television
CBC Cipher block chaining
CLI Command line interface
CM Cable modem
CMCI Cable modem customer interface
CMTS Cable modem termination system
CMTS-MIC Cable modem termination system - message integrity check
CPE Customer premises equipment
DAB Digital Audio Broadcasting
DCC Dynamic channel change (DOCSIS management message)
DES Data encryption standard
DHCPD Dynamic host configuration protocol daemon
DMIC Dynamic message integrity check
DS Downstream
DSP Digital signal processing/processor
DVB Digital Video Broadcasting
EAE Early authentication and encryption
eDOCSIS Embedded DOCSIS
EMC electromagnetic compatibility
EMI electromagnetic interference
EPON Ethernet passive optical network
FCC Federal Communications Commission
FEC Forward error correction
FPGA Field programmable gate array
GPON Gigabit passive optical network
HFC Hybrid fiber coax

HMAC Hashed message authentication code
IC Integrated circuit
ISP In system programming
JTAG Joint Test Action Group
KEK Key encryption key
MAC Medium Access Control
MDD MAC domain descriptor (DOCSIS management message)
MER Modulation error rate
MIB Management Information Base
MIC Message integrity check
MMH Multilinear modular hash
NTSC National Television Systems Committee
NVRAM Non volatile RAM
ODN Optical distribution network
OLT Optical Line Terminal
ONT Optical Network Terminal
ONU Optical Network Unit
PAL Phase Alternating Line
PDU Protocol data unit
PHS Payload header suppression
PHY Physical Layer
PID Packet Identifier
PKI Public Key Infrastructure
PMD Physical Media Dependent
PNM Pro-active network monitoring
PON Passive optical network
QAM Quadrature amplitude modulation
QPSK Quadrature phase shift keying
RF Radio frequency
RFoG Radio frequency over glass
SA Security association
SAID Security association identifier
SAV Source address verification
SCTE Society of Cable Telecommunications Engineers
SDR Software defined radio
SID Service identifier
SNR Signal-noise ratio
SYNC Synchronization
TEK Traffic encryption key
TLV Type-length-value
UCD Upstream channel descriptor
US Upstream

List of Figures

Listings

Bibliography

[1] S.A. Ahson and M. Ilyas. *WiMAX: Standards and Security*. WiMAX Handbook. CRC Press, 2007.

[2] Christian Schindelhauer Amir Alsbih, Felix C. Freiling. A case study in practical security of cable networks. In *Future Challenges in Security and Privacy for Academia and Industry - 26th IFIP TC 11 International Information Security Conference, SEC 2011, Lucerne, Switzerland, June 7-9, 2011.*, pages 92–103, 2011.

[3] Himanshu Arora. Intro to docsis architecture, cm cmts protocol for cable modems. `http://www.thegeekstuff.com/2012/05/Docsis-introduction/`, May 2012. [last visited: 2018-02-12].

[4] Inc. ARRIS Group. Sb6183: Cable signal levels. `http://arris.force.com/consumers/articles/General_FAQs/SB6183-Cable-Signal-Levels`, October 2017. [last visited: 2018-02-12].

[5] A.A. Azzam. *High Speed Cable Modems: Including IEEE 802.14 Standards*. Computer Communications. McGraw-Hill, 1997.

[6] J. Biskup and J. López. *Computer Security - ESORICS 2007: 12th European Symposium On Research In Computer Security, Dresden, Germany, September 24 - 26, 2007, Proceedings*. LNCS sublibrary: Security and cryptology. Springer, 2007.

[7] Bitemytaco. Hacking docsis for fun and profit. `https://www.defcon.org/images/defcon-18/dc-18-presentations/Blake-bitemytaco/DEFCON-18-Blake-bitemytaco-Hacking-DOCSIS.pdf`, 2009. [last visited: 2018-02-12].

[8] Paul Browning. Broadband and remote access technologies, August 2013. [last visited: 2018-02-12].

[9] W.S. Ciciora. *Modern Cable Television Technology: Video, Voice, and Data Communications*. Electronics & Electrical. Elsevier/Morgan Kaufmann Publishers, 2004.

[10] W.S. Ciciora, J. Farmer, and D. Large. *Modern Cable Television Technology: Video, Voice, and Data Communications*. Morgan Kaufmann series in networking. Morgan Kaufmann Publishers, 1999.

[11] USA Cisco Systems, Inc. *Maximum CPE and Host Parameters for the Cisco CMTS*, 0l-1467-08 edition, February 2007.

[12] USA Cisco Systems, Inc. *Cable ARP Filtering*, february 9, 2009 edition, February 2008.

[13] National Instruments Corporation. Sdr-systeme. http://www.ni.com/de-at/shop/select/software-defined-radios-category, June 2017. [last visited: 2018-02-12].

[14] Jonathan Dharmapalan. Top 10 risks in telecommunications 2014. Technical report, 2014.

[15] Greg Kregoski Dr. Nik Dimitrakopoulos, Peter Lampel. Docsis 3.1 – the game changer for cable tv and internet, 2015. [last visited: 2018-02-12].

[16] DSLReports. Sb6190 puma6 tcp/udp network latency issue discussion. https://www.dslreports.com/forum/r31377755-SB6190-Puma6-TCP-UDP-Network-Latency-Issue-Discussion, April 2017. [last visited: 2018-02-12].

[17] Markus Dürmuth and Thorsten Kranz. On password guessing with gpus and fpgas. In *PASSWORDS*, 2014.

[18] Cable Europe. Certification of vendor equipment. http://www.cable-europe.eu/technology/certification-of-vendor-equipment/, January 2017. [last visited: 2018-02-12].

[19] D.R. Evans. The cable access link. http://www.informit.com/articles/article.aspx?p=167851, July 2001. [last visited: 2018-02-12].

[20] Eric Fagan. Docsis : Data over cable service interface specifications. http://docsis.org/, May 2014. [last visited: 2018-02-12].

[21] D. Fellows and D. Jones. Docsis cable modem technology. *Communications Magazine, IEEE*, 39(3):202–209, Mar 2001.

[22] Electronic Frontier Foundation. Eff des cracker machine brings honesty to crypto debate. https://www.eff.org/de/press/releases/eff-des-cracker-machine-brings-honesty-crypto-debate, August 2016. [last visited: 2018-02-12].

[23] Great Scott Gadgets. Hackrf one. https://greatscottgadgets.com/hackrf/, 10 2014. [last visited: 2018-02-12].

[24] Imre Rad Gergely Eberhardt, György Bácsi and Attila Szász. Evaluation report: Security evaluation of the compal broadband networks ch7465lg m̈ercuryn̈odem. https://www.search-lab.hu/media/Compal_CH7465LG_Evaluation_Report_1.1.pdf, 7 2016. [last visited: 2018-02-12].

[25] DCT DELTA GmbH. KABEL-TV Netzwerke: HFC Produkte & MONITORING. http://www.ets-elektro.at/Mediapool/Dokumente/elektrotechnik/DELTA/Katalog_HFC_dt_QII2015.pdf. [last visited: 2018-02-12].

[26] Normann Engineering GmbH. Pct catv abzweiger / catv taps. http://www.normann-engineering.com/products/product_pdf/passives/pct/01_pct_gx_f1_2.pdf, 2016. [last visited: 2018-02-12].

[27] Mark Chapman Gojo Strkic. Management aspects of a hybrid fiber coaxial (hfc) network. http://www.nctatechnicalpapers.com/Paper/1995/1995-management-aspects-of-a-hybrid-fiber-coaxial-hfc-network/download. [last visited: 2018-02-12].

[28] K. Gould and A. Danforth. System and method for managing provisioning parameters in a cable network, January 20 2005. US Patent App. 10/619,262.

[29] C. Grobicki and J. M. Ulm. Unilink as a media access protocol for community cable tv. In *Community Networking, 1995. Integrated Multimedia Services to the Home., Proceedings of the Second International Workshop on*, pages 41–48, Jun 1995.

[30] Ryan Harris. *Hacking the Cable Modem: What Cable Companies Don't Want You to Know*. No Starch Press Series. No Starch Press, 2006.

[31] Ron Hranac. Catv leakage. http://www.arrl.org/files/file/Technology/CATV%20Leakage.pdf. [last visited: 2018-02-12].

[32] Ron Hranac. Docsis 3.0. Technical report, SCTE, 2006.

[33] ACI Communications Inc. Outdoor cable modem line monitors. http://www.manufacturers.com.tw/showroom-8773-1-5-0000090121-3401.php, October 2017. [last visited: 2018-02-12].

[34] Cable Television Laboratories Inc. *Data-Over-Cable Service Interface Specifications: Baseline Privacy Interface Specification*, sp-bpi-c01-011119 edition, 2001.

[35] Cable Television Laboratories Inc. *Data-Over-Cable Service Interface Specifications: Cable Modem to Customer Premise Equipment Interface Specification*, sp-cmci-i07-020301 edition, March 2002.

[36] Cable Television Laboratories Inc. *Data-Over-Cable Service Interface Specifications (DOCSIS 1.1): Radio Frequency Interface Specification*, cm-sp-rfiv1.1-c01-050907 edition, 2005. [last visited: 2018-02-12].

[37] Cable Television Laboratories Inc. *Data-Over-Cable Service Interface Specifications: Baseline Privacy Plus Interface Specification*, cm-sp-bpi+-c01-081104 edition, 2008.

[38] Cable Television Laboratories Inc. *Data-Over-Cable Service Interface Specifications: Cable Modem to Customer Premise Equipment Interface*, cm-sp-cmci-c01-081104 edition, November 2008.

[39] Cable Television Laboratories Inc. *Data-Over-Cable Service Interface Specifications (DOCSIS 2.0): Operations Support System Interface Specification*, c01-081104 edition, November 2008.

[40] Cable Television Laboratories Inc. *Data-Over-Cable Service Interface Specifications: Radio Frequency Interface Specification*, cm-sp-rfiv2.0-c02-090422 edition, 2009.

[41] Cable Television Laboratories Inc. *Data-Over-Cable Service Interface Specifications: Security Specification*, cm-sp-secv3.0-i15-130808 edition, 2013.

[42] Cable Television Laboratories Inc. *Data-Over-Cable Service Interface Specifications: MAC and Upper Layer Protocols Interface Specification*, cm-sp-mulpiv3.1-i27-150528 edition, May 2015.

[43] Cable Television Laboratories Inc. *DOCSIS Best Practices and Guidelines: PNM Best Practices: HFC Networks (DOCSIS 3.0)*, v03-160725 edition, July 2016.

[44] Cable Television Laboratories Inc. Certification - cablelabs. `http://www.cablelabs.com/specs/certification/`, January 2017. [last visited: 2018-02-12].

[45] Cable Television Laboratories Inc. *Data-Over-Cable Service Interface Specifications: MAC and Upper Layer Protocols Interface Specification*, cm-sp-mulpiv3.1-i10-170111 edition, 2017.

[46] Cisco Systems Inc. Configuring dhcp, tod, tftp services on cisco's cmts: All-in-one configuration, document id:28990. `http://www.cisco.com/c/en/us/support/docs/broadband-cable/cable-modem-termination-systems-cmts/28990-all-in-one-config.html`, November 2006. [last visited: 2018-02-12].

[47] Cisco Systems Inc. Docsis load balancing groups. `https://www.cisco.com/c/en/us/td/docs/cable/cbr/configuration/guide/b_cbr_layer2_docsis/docsis_load_balancing_groups.pdf`, 4 2015. [last visited: 2018-02-12].

[48] Cisco Systems Inc. Dynamic shared secret for the cisco cmts routers. `https://www.cisco.com/c/en/us/td/docs/cable/cmts/config_guide/b_cisco_cmts_scg/b_cisco_cmts_scg_chapter_0111101.pdf`, 11 2015. [last visited: 2018-02-12].

[49] NETGEAR Inc. Docsis 3.1 technology whitepaper, 2016. [last visited: 2018-02-12].

[50] Sencore Inc. Slm 1479 portable cable/digital tv rf analyzer. `http://www.sencore.com/sites/default/files/SLM1479.pdf`, 2016. [last visited: 2018-02-12].

[51] Deviser Instruments Incorporated. Ds2500q digital tv qam analyzer. http://www.devisertek.com/uploads/3/4/7/9/34796732/ds2500q_datasheet_160113.pdf, 2016. [last visited: 2018-02-12].

[52] A. Keller. *Datenübertragung im Kabelnetz: DOCSIS über Hybrid-Fibre-Coax*. Springer Berlin Heidelberg, 2005.

[53] Andres Keller. Docsis. In *Breitbandkabel und Zugangsnetze*, pages 327–391. Springer Berlin Heidelberg, 2011.

[54] Shivani Kundu Khushboo, Swati Garg. Internet access via cable tv network. Technical report, COMPUTER SCIENCE and ENGINEERING, Uttar Pradesh Technical University, 2014.

[55] Constantinos Kolias, Georgios Kambourakis, and Stefanos Gritzalis. Attacks and countermeasures on 802.16: Analysis and assessment. 15:487–514, 01 2013.

[56] Benjamin Larsson. Linuxtv patchwork rtl28xxu: lower the rc poll time to mitigate i2c transfer errors. https://patchwork.linuxtv.org/patch/27348/, December 2014. [last visited: 2018-02-12].

[57] M.E. Laubach, D.J. Farber, and S.D. Dukes. *Delivering Internet Connections over Cable: Breaking the Access Barrier*. Networking Council. Wiley, 2002.

[58] Dexter Lindstrom. Sniffing a cable modem network: Possible or myth?, March 2002. [last visited: 2018-02-12].

[59] David Longenecker. Arris (motorola) surfboard modem unauthenticated reboot flaw. https://www.securityforrealpeople.com/2016/04/arris-motorola-surfboard-modem.html, 4 2016. [last visited: 2018-02-12].

[60] Wen-Pai Lu. An overview of link security– protocols and standards, February 2004. [last visited: 2018-02-12].

[61] Dolors Sala Mahalingam Mani. Comparative analysis of link security mechanisms. Technical report, Avaya, Broadcom, 2002.

[62] Guy Martin. Sniffing cable modems. http://www.packet-o-matic.org/downloads/talks/sniffing-cable-modems-hackcon4.odp, 2009. [last visited: 2018-02-12].

[63] Guy Martin. Getting started: Processing steps. https://wiki.packet-o-matic.org/pom-ng/getting_started, January 2013. [last visited: 2018-02-12].

[64] Guy Martin. Docsis sniffing notes. https://wiki.packet-o-matic.org/pom-ng/docsis/docsis, June 2014. [last visited: 2018-02-12].

[65] Guy Martin. Installing pom-ng. https://wiki.packet-o-matic.org/pom-ng/installation, January 2016. [last visited: 2018-02-12].

[66] Tadauchi Masaharu, Ishii Tatsuei, and Itoh Susumu. A mac-layer security architecture for cable networks. In Borka Jerman-Blažič and Tomaž Klobučar, editors, *Advanced Communications and Multimedia Security*, volume 100 of *IFIP — The International Federation for Information Processing*, pages 79–90. Springer US, 2002.

[67] Curtis Knittle Matt Schmitt. Dpoe overview, March 2012. [last visited: 2018-02-12].

[68] Hector Mayorga. Epon and rfog technology overview, 2015. [last visited: 2018-02-12].

[69] J.T. McKelvey. Combating security risks on the cable ip network. `http://svc003.wic723dp.server-web.com/whitepapers/IBCCiscoSecurityCableIP.pdf`. [last visited: 2018-02-12].

[70] M. Millet and A. Thomas. Method and system for cloned cable modem detection, May 11 2010. US Patent 7,716,468.

[71] MITRE. Cve-2015-7289. `https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7289`, 9 2015. [last visited: 2018-02-12].

[72] MITRE. Cve-2017-9521. `https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9521`, 6 2017. [last visited: 2018-02-12].

[73] Scott Moser and James J. Martin. Assessing denial of service vulnerabilities in docsis. In *ACM Southeast Regional Conference*, 2006.

[74] RICHARD MURPHY. A simulation study of docsis upstream channel bandwidth allocation strategies for minimal user response time. Master's thesis, THE UNIVERSITY OF TEXAS AT SAN ANTONIO, College of Sciences, Department of Computer Science, 12 2004.

[75] Demetres Kouvatsos Neel Shah. A tutorial on docsis: Protocol and models. Technical report, Clemson University, 2005.

[76] Shaun Nichols. Intel pumageddon: Broadband chip bug haunts chipzilla's past, present and future: You can trivially dos puma 5 and 7-powered boxes, too. `http://www.theregister.co.uk/2017/08/09/intel_puma_modem_woes/`, August 2017. [last visited: 2018-02-12].

[77] Shaun Nichols. Intel's buggy puma 6 chipset earns arris a gigabit-modem lawsuit. `https://www.theregister.co.uk/2017/04/11/intel_puma_6_arris/`, April 2017. [last visited: 2018-02-12].

[78] The SRLabs Team (Karsten Nohl). Rooting sim cards. `https://media.blackhat.com/us-13/us-13-Nohl-Rooting-SIM-cards-Slides.pdf`, July 2013. [last visited: 2018-02-12].

[79] Pierluigi Paganini. Hacking 4g usb modems and sim card via sms. http://securityaffairs.co/wordpress/31663/hacking/hacking-4g-usb-modems.html, December 2014.

[80] Antti Palosaari. Naked hardware #14: Dvb-t2 usb tv stick hd-901t2. http://blog.palosaari.fi/2013/10/naked-hardware-14-dvb-t2-usb-tv-stick.html, October 2013. [last visited: 2018-02-12].

[81] Sylvain Pelissier. Do not create a backdoor, use your provider's one ! https://research.kudelskisecurity.com/2017/01/06/do-not-create-a-backdoor-use-your-providers-one/, 1 2017. [last visited: 2018-02-12].

[82] Annie Phan. Securing docsis cable networks. Technical report, Industry Affairs Department, 2002.

[83] J. Postel and K. Harrenstien. RFC 868: Time protocol, May 1983.

[84] Rafael Micro. *R820T High Performance Low Power Advanced Digital TV Silicon Tuner*, 11 2011. 1.2.

[85] Bernardo Rodrigues. Unpacking firmware images from cable modems last checked: 2018-02-07. https://w00tsec.blogspot.co.at/2013/11/unpacking-firmware-images-from-cable.html, November 2013. [last visited: 2018-02-12].

[86] Bernardo Rodrigues. Arris cable modem has a backdoor in the backdoor. https://w00tsec.blogspot.co.at/2015/11/arris-cable-modem-has-backdoor-in.html, 11 2015. [last visited: 2018-02-12].

[87] Bernardo Rodrigues. Hacking cable modems the later years. https://github.com/bmaia/slides/raw/master/nullbyte_2015-hacking_cable_modems_the_later_years.pdf, 2015. [last visited: 2018-02-12].

[88] Bernardo Rodrigues. Luabot: Malware targeting cable modems. https://w00tsec.blogspot.co.at/2016/09/luabot-malware-targeting-cable-modems.html, 9 2016. [last visited: 2018-02-12].

[89] Mark Goodman Rolando Domdom, Brian Espey. A simulation analysis of the initialization of docsis-compliant cable modem systems. Technical report, Department of Systems Engineering, University of Virginia, 2000.

[90] RSA Security. A guide to securing broadband cable networks: Docsis security. Technical report, techguide.com, 2001.

[91] Kristof Sercu. The differences between us docsis and eurodocsis, and will docsis 3.1 eliminate them? https://www.excentis.com/blog/differences-between-us-docsis-and-eurodocsis-and-will-docsis-31-eliminate-them, October 2014. [last visited: 2018-02-12].

[92] Joel Stein. Hacking docsis. https://events.ccc.de/congress/2016/wiki/images/9/92/33c3_Hacking_DOCSIS.pdf, 12 2016. [last visited: 2018-02-12].

[93] Packet Storm. 802.14 and docsis standard information. https://dl.packetstormsecurity.net/papers/evaluation/docsis/cable.html, August 2000.

[94] Karthik Sundaresan. Evolution of cmts/ccap architectures. Technical report, Cable Television Laboratories Inc, 2015.

[95] Cisco Systems. *Cisco uBR7200 Series Universal Broadband Router Hardware Installation Guide Appendix B: RF Specifications*, 2003.

[96] Braden Thomas. Cabletables. https://bitbucket.org/drspringfield/cabletables, April 2015. [last visited: 2018-02-12].

[97] Braden Thomas. Practical attacks on docsis. https://bitbucket.org/drspringfield/cabletables/downloads/PracticalAttacksOnDOCSIS.pdf, April 2015. [last visited: 2018-02-12].

[98] Kabelnetze für Fernsehsignale, Tonsignale und interaktive Dienste – Teil 1: Systemanforderungen in Vorwärtsrichtung, February 2009.

[99] Brady Volpe. Docsis and cable modems – how it works :: Cable modem registration. https://volpefirm.com/docsis-cable-modem-registration/, September 2009. [last visited: 2018-02-12].

[100] Brady Volpe. Zcorum's ask a broadband expert series: Docsis pre-equalization: Vastly powerful, often undervalued. http://www.zcorum.com/wp-content/uploads/Pre-Equalization-Final.pdf, January 2014. [last visited: 2018-02-12].

Curriculum Vitae

Personal data

Name	Christian Voglhuber
Date of birth	July 31, 1990
Family status	Married
Citizenship	Austria
Parents	Johann Voglhuber Margarida Voglhuber

Professional experience

2013-2017	IT and electronics engineer, FAME Technologies GmbH (Linz)
since 2010	IT and electronics engineer, Voglhuber GmbH (Petzenkirchen)
since 2013	CEO, Voglhuber GmbH (Petzenkirchen)

Education

1996–2000	Primary school Petzenkirchen
2000–2004	Computer-Hauptschule Wieselburg
2004–2009	IT-HTL Ybbs an der Donau, Subject: Network Technology
June 2009	School leaving certificate (Matura)
since 2010	Study of computer science at Johannes Kepler University Linz

Statutory declaration

I hereby declare that the thesis submitted is my own unaided work, that I have not used other than the sources indicated, and that all direct and indirect sources are acknowledged as references.

This printed thesis is identical with the electronic version submitted.

Linz, 7.5.2018

Signature